Product Roundup: Event Log Managers p. 49

# Windows® IT Pro

NOVEMBER 2009 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

# AD GOLD!

Mine These Lesser-Known Active Directory Tools p. 25

## Windows Server 2008 R2
New AD Features p. 29

## Exchange Server 2007
Transport Rules and Message Classifications p. 34

Round Up Those Scripts p. 39

Spice Up SharePoint Search Results p. 42

## Need to Know
Hyper-V 2.0 p. 10

PENTON
A PENTON PUBLICATION
NOVEMBER 2009
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

# Kiss your antivirus bloatware goodbye

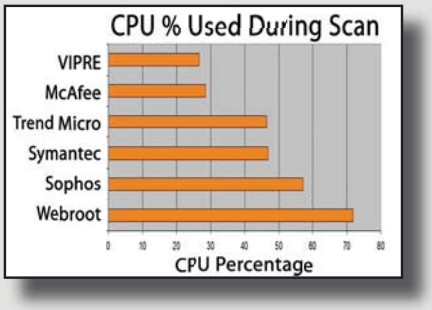
**Special Competitive Upgrade Price: $10 per seat!**

## TEST DRIVE

# VIPRE® ENTERPRISE

## Next Generation of Total Malware Protection

The configurable Command Center puts all the information you need in one place. Manage individual agents, quarantines, threats, and more.




How does your current software compare? VIPRE Enterprise scans at a brisk 13.95 MB/sec and uses just 27% of CPU and 50 MB of RAM. In idle, it uses a mere 13.3 MB RAM with a disk footprint of just 113 MB. You'll hardly notice it's running!

Sunbelt Software

**Until now, antivirus engines have been Frankensteins, bolted together from bits and pieces of different products.** They're slow, full of bugs, and hard to manage.

VIPRE Enterprise is a revolutionary new approach. It's built from scratch as the all-in-one antivirus, antispyware, anti-rootkit solution that gives you complete endpoint malware protection ***without hogging resources!*** It's fast, powerful, and easy.

Plus, advanced anti-malware technology protects your system against the new wave of malware threats. No more juggling multiple programs. No more dealing with user complaints about slow workstation performance.

- **COMPLETE!** All-in-one protection from today's malware.
- **FAST!** High-performance and low impact on system resources.
- **EASY!** Manage everything easily from one command screen.
- **RELIABLE!** Configurable, real-time monitoring technology.
- **AFFORDABLE!** Low $10 per seat pricing to save you money.

Why struggle with slow resource hogs when you can manage ALL your malware threats with one fast, easy application?

**Curious? Download your FREE copy of VIPRE Enterprise and give it a test drive.**

When you compare VIPRE Enterprise to Symantec, McAfee, Trend Micro or whatever antivirus program you're using, **you WILL want to switch!** Don't worry, though.You can get VIPRE Enterprise at our competitive upgrade price of **only $10 per seat!**

**Download VIPRE Enterprise today and get your own home version of VIPRE to keep FREE as our gift to you!**

**Download now: www.TestDriveVipre.com**

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.SunbeltSoftware.com sales@sunbeltsoftware.com



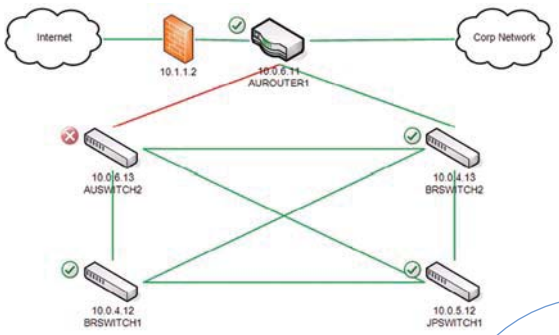
New licenses are available for $10/seat up to 500 seats, minimum 10 seats. For customers with over 500 seats, please call for special pricing. Available for a limited time and subject to change without notice. See website for more details.

savision

FREE VERSION AVAILABLE!

# See More. Know More. Do More.

Live Maps for Operations Manager 2007 enables employees at all levels, from the IT operator to business executive, to **see more** context for every IT problem. Live Maps allows IT organizations to rapidly conceive, build and maintain large-scale monitoring maps in order to **know more** about how IT problems affect business operations. This allows IT pros everywhere to **do more** with less.





## Live Maps

for Operations Manager 2007

+

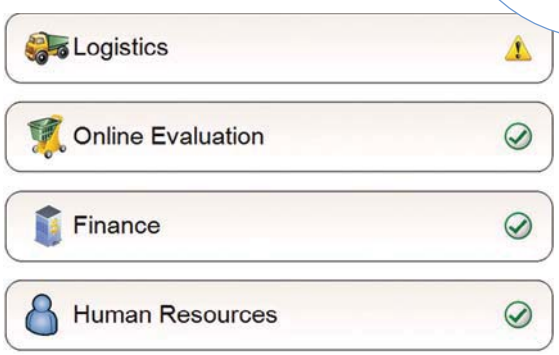
Microsoft® System Center Operations Manager 2007

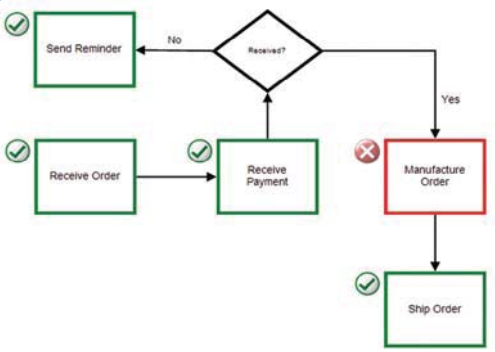
**Application & Network Topologies**

**Geographical Views**

**IT and Service Dashboards**

**Business Process Monitoring**




To learn more about Savision's products and services or to download a free copy, visit www.savision.com. US & International Sales: +31 30 2442351 or sales@savision.com.

Microsoft CERTIFIED Partner

Get your free copy at **www.savision.com/free**


# NO-NONSENSE WEB FILTERING

That's what you'll get when you switch to iPrism from St Bernard – the award-winning web filter that's easier in every way, and less expensive to own.

iPrism is changing the way companies and schools everywhere handle their web filtering. With blazing throughput speeds up to 100+ Mbps, anti-virus protection and seamless XenApp and Active Directory integration, iPrism is the appliance-based solution of choice for customers and institutions of any size.

Find out more about the easiest-to-deploy, most highly rated web filtering solution ever – the industry's ONLY Citrix-ready web filtering appliance.

**Call 1.800.782.3762 or go to www.SwitchToiPrism.com**

ST BERNARD

## FLIP THE SWITCH

Get your FREE iPrism® Switch Kit today:

**FREE 30-day onsite evaluation**
that can be deployed without any client or network changes

**FREE enhanced technical support**
for setting up matching policies, reports & alerts based on your current settings

**INCENTIVE PRICING & A FREE T-SHIRT**
just for watching a live demo

iPrism® h-Series, the world's #1 Web Filtering appliance.

# CONTENTS


## COVER STORY



## FEATURES



## INTERACT



## PRODUCTS




Windows IT Pro
A PENTON PUBLICATION
NOVEMBER_2009
VOLUME_15
NO_11


## COLUMNS



Access articles online at www.windowsitpro.com.
Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

# CONTENTS

## IN EVERY ISSUE



## ON THE WEB

Read these articles at www.windowsitpro.com.

### Windows Gatekeeper

Show users failed log on attempts as a security measure, harden Exchange 2007 servers with Security Configuration Wizard, and determine whether a user has logged on using a smart card.

—Jan De Clercq

InstantDoc IDs 102843, 102844, 102845

### Outlook Tips & Techniques

Open Outlook 2007 directly to your to do list, learn what Outlook 2007 with BCM is, and find out how to defrag workstations to improve Outlook performance.

—William Lefkovics

InstantDoc IDs 102861, 102862, 102863

### ACL Enhancements in Windows Vista and Windows Server 2008

ACL changes in the Windows OS aren't game-changing, but a strong understanding of the small modifications can help simplify security management and resolve permissions-related problems in your environment.

—Russell Smith

InstantDoc ID 102871

### New Ways to Reach *Windows IT Pro* Editors

**Twitter:** Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

**LinkedIn:** To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

**Facebook:** We've created a page on Facebook for *Windows IT Pro*, which you can access at http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.


Windows IT Pro

## EDITORIAL

**Editorial and Custom Strategy Director**
Michele Crockett mcrockett@windowsitpro.com

**Editor-in-Chief, Web Content Strategist**
Jeff James jjames@windowsitpro.com

**Executive Editor, IT Group**
Amy Eisenberg amy@windowsitpro.com

**Technical Director**
Michael Otey motey@windowsitpro.com

**Custom Group Editorial Director**
Dave Bernard dbernard@windowsitpro.com

**Web and Developer Strategic Editor**
Anne Grubb agrubb@windowsitpro.com

**Systems Management**
Karen Bemowski kbemowski@windowsitpro.com
Caroline Marwitz cmarwitz@windowsitpro.com
Zac Wiggy zwiggy@windowsitpro.com

**Messaging , Mobility, SharePoint, and Office**
Brian Keith Winstead bwinstead@windowsitpro.com

**Networking and Hardware**
Jason Bovberg jbovberg@windowsitpro.com

**Security**
Lavon Peters lpeters@windowsitpro.com

**SQL Server**
Megan Bearly Keller mkeller@windowsitpro.com
Sheila Molnar smolnar@windowsitpro.com

**Production Editor**
Brian Reinholz breinholz@windowsitpro.com

**IT Media Group Editors**
Linda Harty, Chris Maxcer, Rita-Lyn Sanders

## CONTRIBUTORS

**News Editor**
Paul Thurrott news@windowsitpro.com

**SharePoint and Office Community Editor**
Dan Holme danh@intelliem.com

**Senior Contributing Editors**
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com

**Contributing Editors**
Alex K. Angelopoulos aka@mvps.org
Sean Deuby sdeuby@windowsitpro.com
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond tony.redmond@hp.com
Ed Roth eroth@windowsitpro.com
Eric B. Rux ericbrux@whshelp.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

## ART & PRODUCTION

**Senior Art Director**
Larry Purvis lpurvis@windowsitpro.com

**Art Director**
Layne Petersen layne@windowsitpro.com

**Production Director**
Linda Kirchgesler linda@windowsitpro.com

**Senior Production Manager**
Kate Brown kbrown@windowsitpro.com

**Assistant Production Manager**
Erik Lodermeier erik.lodermeier@penton.com

## ADVERTISING SALES

**Publisher** Peg Miller pmiller@windowsitpro.com

**EMEA Managing Director** Irene Clapham irene.clapham@penton.com

**Director of Sales** Birdie J. Ghiglione birdie.ghiglione@penton.com, 619-442-4064

**Online Sales and Marketing Manager** Dina Baird Dina.Baird@penton.com

**Key Account Directors**
Jeff Carnes jeff.carnes@penton.com 678-455-6146
Chrissy Ferraro christina.ferraro@penton.com 970-203-2883
Jacquelyn Baillie jacquelyn.baillie@penton.com 714-623-5007

**Account Executives**
Barbara Ritter barbara.ritter@penton.com 858-759-3377
Cass Schulz cassandra.schulz@penton.com 858-357-7649

**Client Project Managers**
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

**Ad Production Supervisor**
Glenda Vaught glenda.vaught@penton.com

## MARKETING & CIRCULATION

**Customer Service** 800-793-5697 (US and Canada) 44-161-929-2800 (Europe)

**IT Group Audience Development Director**
Marie Evans marie.evans@penton.com

**Marketing Director**
Sandy Lang sandy.lang@penton.com

## CORPORATE

PENTON

**Chief Executive Officer**
Sharon Rowlands Sharon.Rowlands@penton.com

**Chief Financial Officer/Executive Vice President**
Jean Clifton jean.clifton@penton.com

## TECHNOLOGY GROUP

**Senior Vice President, Technology Media Group**
Kim Paulsen kpaulsen@windowsitpro.com




**WRITING FOR *WINDOWS IT PRO***

Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.



**LIST RENTALS**

Contact Walter Karl, Inc. at 2 Blue Hill Plaza, 3rd Floor, Pearl River, NY 10965 or www.walterkarl.com/mailings/pentonLD/index.html.

**REPRINTS**

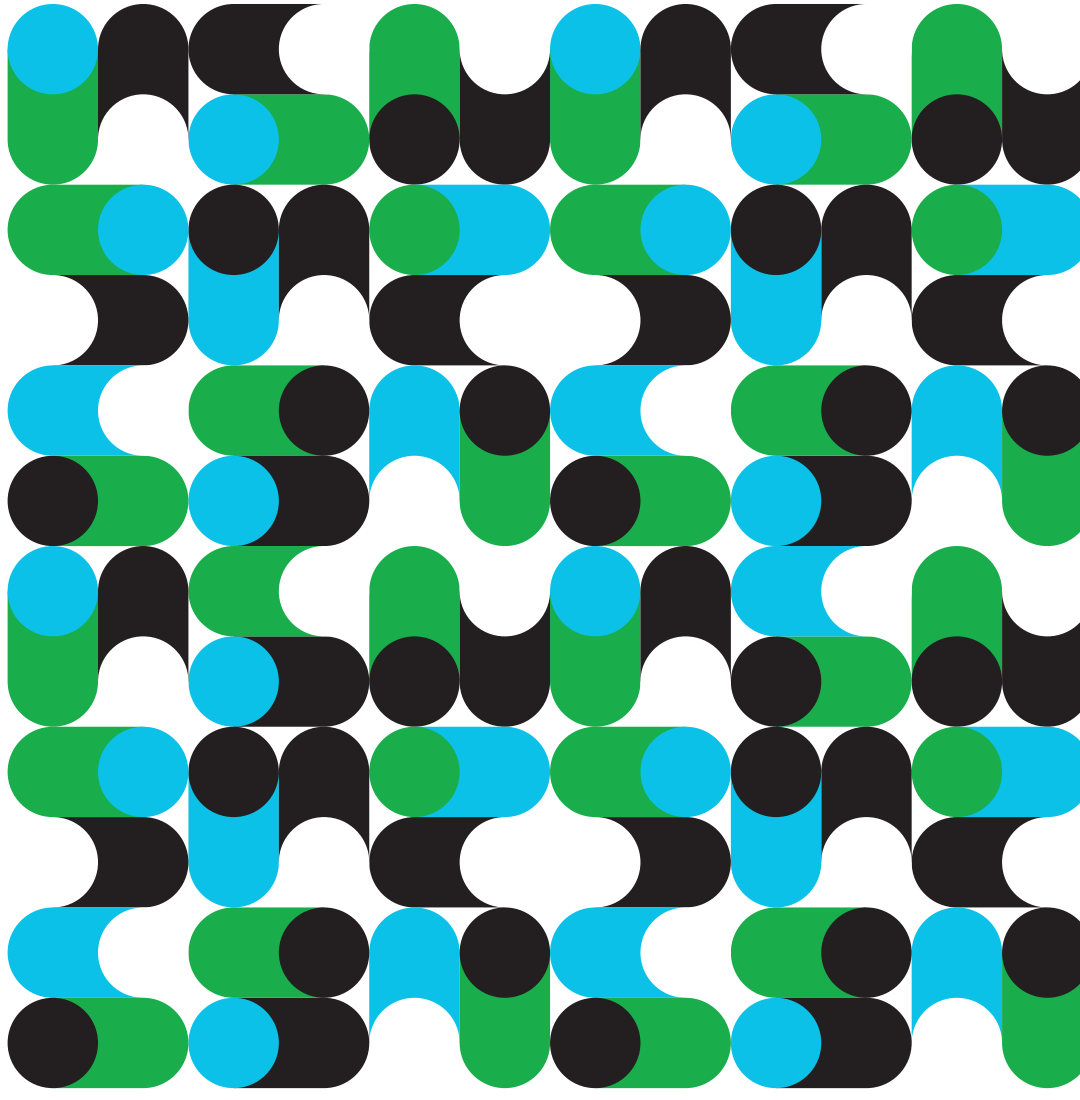
Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

Smarter technology for a Smarter Planet:

# Can an entire business be given a nervous system?

On a smarter planet, the datacenter is not simply the heart of IT—it's also the central nervous system of the entire business. IBM is helping companies view their extended infrastructure not as a collection of disconnected pieces, but as an integrated system that connects the datacenter to all of the digital and physical assets of the business, creating a more dynamic infrastructure. From railway systems that can predict and schedule their own maintenance to assembly lines that understand how to adjust to changing needs to power grids that match supply and demand, we're already helping customers improve service, increase flexibility and reduce operating costs by as much as 50%.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/infrastructure



# Crockett

"IT purchases for 2010 must show immediate and compelling bottom-line savings."

# Window Shopping for 2010 IT Purchases

## Windows 7 deployment will likely surpass Server 2008 R2 and Exchange 2010

Microsoft's three-way product launch this fall of Windows 7, Windows Server 2008 R2, and Exchange Server 2010 is a refreshing burst of activity in an otherwise stagnant product launch year. But talking about a product, getting a demo about a product, or even craving a product isn't the same as actually buying a product. (Probably only Windows 7 stirs any emotion remotely resembling a craving.)

According to our recent independently conducted audience research, as the economically painful 2009 winds to a close, businesses will continue to hold tight to their cash. New technology whose primary benefit is the cool factor isn't high on any IT manager's shopping list unless keeping his or her job also isn't top on the list. All of the future efficiencies promised by new technology will be seriously weighed against turning in decent business performance this last quarter. But that doesn't mean we all can't do a little window shopping for 2010 purchases that will achieve some efficiency benefits. The problem is finding the clear-cut efficiencies that will really make a difference in the short term.

### Deployment Plans

The clear winner among our readers in the plan-to-deploy race is Windows 7. Among our print, email, and web audience, about 58 percent of respondents indicated that they plan to deploy Windows 7 in 2010. Favorite Windows 7 features that are driving this anticipation include faster boot times, an improved UI, and the Windows XP mode (yes, there is irony in that last one). For Paul Thurrott's discussion of the Windows 7 launch and some audience reaction to the release, check out "Windows 7 Will Set Industry Afire" (windowsitpro.com, InstantDoc ID 102819). Interestingly, even the promise of excising Vista isn't enough for some of our readers to jump on Windows 7, primarily because they never deployed Vista in the first place.

Server 2008 R2 shows decent potential for deployment in 2010 as well. Only about 48 percent of our audience currently has Server 2008 running somewhere in the organization. A little over half of respondents indicated plans to deploy Server 2008 R2 in 2010. But for those who are squeamish about deployment, the admittedly intriguing features such as the 64-bit capability make the decision even tougher. Cash-strapped companies that don't already have 64-bit hardware are going to have to wait. The new Live Migration feature that lets you move Hyper-V virtual machines (VMs) between hosts with no downtime is great. But most of our readers who are currently using virtualization technology already have VMware implementations in place. (For Michael Otey's quick picks of the most compelling Server 2008 R2 features, check out "New Features in Windows Server 2008 R2," windowsitpro.com, InstantDoc ID 101470.)

The statistics regarding Exchange Server migration tell the classic if-it-ain't-broke-don't-fix-it story. About 46 percent of our audience uses Exchange Server 2003. Only about 33 percent of respondents have deployed Exchange Server 2007. And only about 32 percent of our audience plans to deploy Exchange 2010 within six months after release. For those who've looked at Exchange 2010, the winning features are built-in email archiving and Database Availability Groups (DAGs) for improved high availability. But of those readers who have no plans to upgrade, the top reasons cited for holding tight to previous versions are that they're unconvinced about the benefits of migrating, they don't have the budget, or it's simply been too soon since their last upgrade. And forget about unified communications (UC) driving adoption: Less than 8 percent of our audience have deployed any form of UC. According to comments from our Instant Polls, most readers see UC as too expensive and too complicated. In fact, a recent Instant Poll asking about Microsoft Office Communications Server (OCS) adoption elicited the most votes for the response, "What the heck is OCS?" For basic Exchange Server migrations, the angst is real as many organizations struggle with when and how to move from Exchange 2003, which has quietly and relatively seamlessly served up email in organizations for years. Paul Robichaux offers some excellent advice in "Exchange 2007 Now or Exchange 2010 Later?" (windowsitpro.com, InstanstDoc ID 102197).

### Hats Off to Windows 7

So as we put the wrapper on this decidedly underwhelming IT buying year, let's all give a little salute to Windows 7 for causing some checkbooks to come out of the drawer. For most companies, IT purchases for 2010 must show immediate and compelling bottom-line savings. Bells and whistles, anyone? I didn't think so.

InstantDoc ID 102833

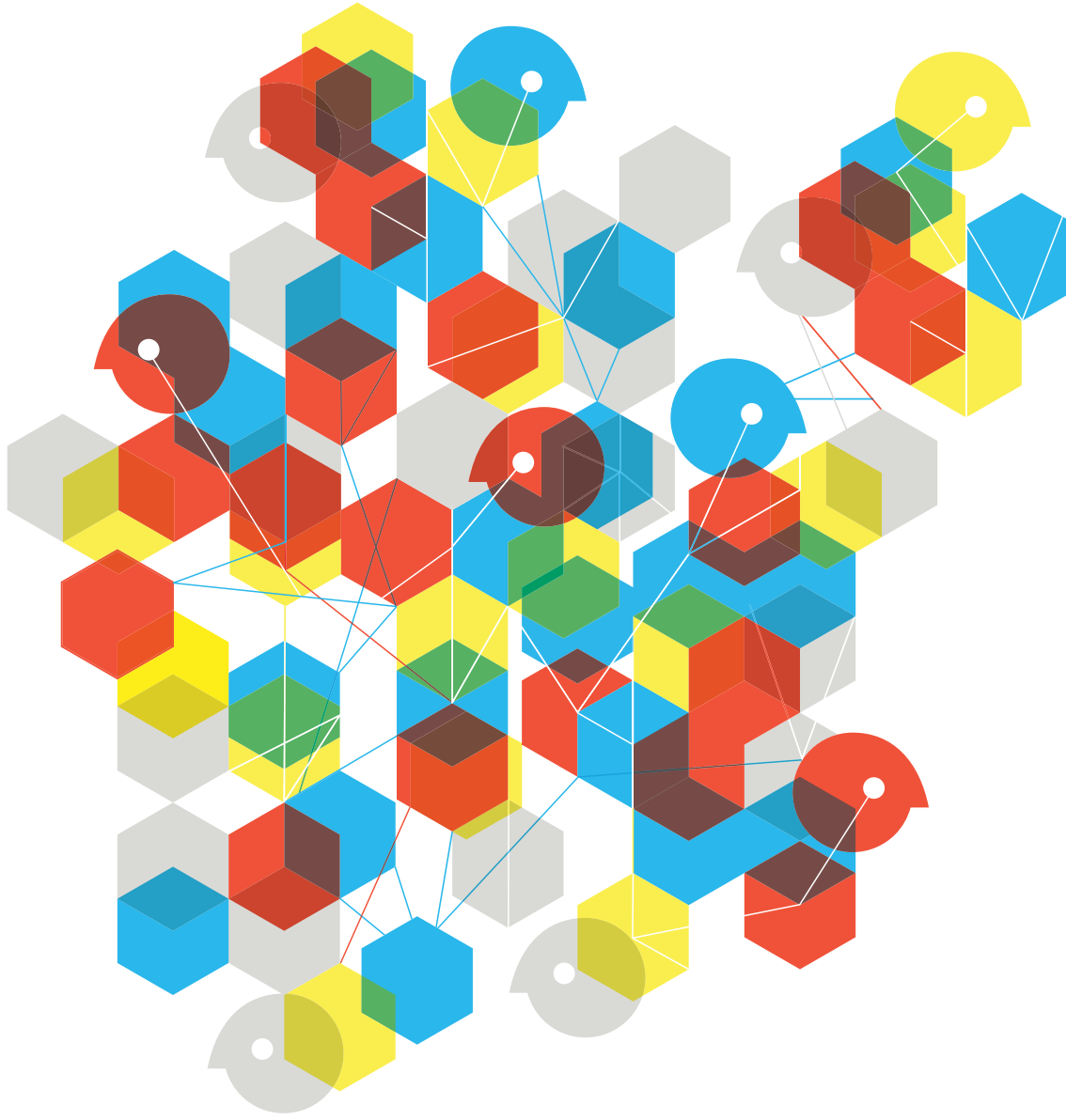
**MICHELE CROCKETT** (michele.crockett@penton.com) helped launch *SQL Server Magazine* in 1999, has held various business and editorial roles within Penton Media, and is currently editorial and custom strategy director of *Windows IT Pro*, *SQL Server Magazine*, and *SystemiNetwork*.

Smarter technology for a Smarter Planet:

# Can the boundaries of a business be defined by its people instead of its walls?

On a smaller, flatter, smarter planet, we increasingly find ourselves working with people far outside the walls of the enterprise: partners, suppliers, customers and remote employees. IBM is incorporating new tools, like social software, wikis and presence awareness, throughout our collaboration portfolio—as well as new ways of accessing these tools through the cloud. Cloud-based solutions like LotusLive™ let your people work with whomever they want, regardless of what side of the firewall they're on. All backed by the legendary security you expect from IBM. Now you can extend your collaboration infrastructure without the cost and complexity of additional infrastructure. So you don't have to tear down your walls to reach beyond them.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/collaborate



- PowerShell Script
- Free Utilities
- EU Ease-Up
- Microsoft Support

## LETTERS@WINDOWSITPRO.COM

### Rebooting with PowerShell

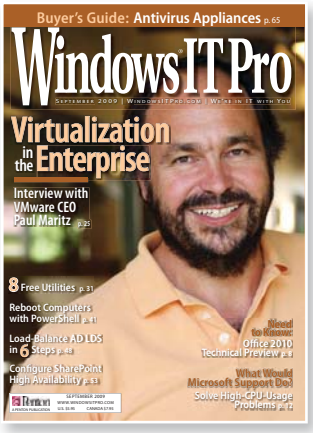
Thanks to Bill Stewart ("Rebooting Computers Using PowerShell," September 2009, InstantDoc ID 102361) for a great script! This script will help me reboot hundreds of servers after patching them.

—Matthew Van Den Bos

### Keep Sharing Those Free Utilities!

Douglas Toombs presents an excellent selection of Windows utilities in "8 More Excellent Free Utilities" (September 2009, InstantDoc ID 102446). I've been playing with WinAudit in conjunction with WinDiff. I have WinAudit pull the system files into a .csv file prior to patching. I rescan after the patch update, then use WinDiff to compare the two files. My only problem is that the process doesn't seem to work properly in Windows 7, so I'm investigating that.

I remember reading Toombs' "Mail Filtering with Fluffy the SMTP-GuardDog" (August 2004, InstantDoc ID 43204). At the time, I was using Exchange Server 2003 on Windows 2003 Server at home. I enjoyed looking at the logs to see who was spamming me. Then I found out about spamhaus.org, a site that offered a DNS blacklist for home use. (Spamhaus .org is free for home users running Exchange 2000 or 2003, but corporations need to pay for it.)




I configured Fluffy to receive mail on port 25 and pass it to the Exchange on port 26—a scenario that worked great with the spamhaus.org-housed DNS blacklist as long as I was running Exchange 2003 or 2000. I could configure Exchange to provide an Edge Transport server role in the DMZ that passes mail to the back-end Exchange server via a certificate-authenticated link. Then came Exchange 2007, which offered the same (if not more) capabilities than Fluffy did. Setting up Fluffy as the email entrance point didn't work with Exchange 2007; I couldn't figure how to set the Edge Transport server to pass mail to the back-end server via port 26.

Anyway, I've used *Windows IT Pro* many times to enhance my collection of tips, tricks, and utilities, and Doug's articles are always great sources of information. Keep up the good work!

—Bill Crouch

### Ease Up on EU

I'm a long-time reader of Paul Thurrott's WinInfo newsletter, and I greatly appreciate his excellent views on all IT matters. However, his stance in "Google Scrambles to Appease EU Regulators over Book Scanning" (September 8, 2009, InstantDoc ID 102776) regarding "overly aggressive European Union antitrust regulators" is getting a bit tiresome.

I have no problem with the EU investigating anyone, as many times as necessary, as long as the outcome is just. I don't follow the EU cases as closely as Paul does, but the only case I think the EU got wrong was the Internet Explorer (IE) bundling case. However, that was on the back of Microsoft's bullying of PC makers.

My problem with EU regulators is that they don't apply the same level of scrutiny and standards to other companies. I'm thinking of Apple and Google. If you're going to beat EU regulators with a stick, beat them with the correct stick, please!

The Google book-scanning case is probably the trickiest of the lot because it covers differing copyright laws in every country. Ultimately, the concern involves freedom of information. I can go to a local library and get just about any book I want. Google is aiming for that kind of accessibility, but the library offers it for free, non-profit, for the common educational goal of "books for everyone, for free." One company I worked for had a small library that was connected to the local public library, offering book shares and book rotation.

I'm generally not a fan of government-run organizations. However, if the alternative is Google holding all the keys to all the books, I'd prefer a government-run (or even a United Nations Educational, Scientific and Cultural Organization—UNESCO—run) organization. Then again, I wouldn't trust either Google or the UN to open a can of baked beans.

I hope this letter doesn't come across as a bash. Please keep up the truly brilliant work, Paul.

—Mark Gillard
InstantDoc ID 102823

### Microsoft Supports Microsoft Support

I read your "What Would Microsoft Support Do?" column every month, and I really like the tips that it provides. The September article about ProcDump ("Got High-CPU Usage Problems? ProcDump 'Em!" InstantDoc ID 102479) is very cool. I referenced this article in my personal blog on TechNet (blogs.technet.com/yuridiogenes/archive/2009/09/01/wspsrv-exe-causing-random-high-cpu-utilization-how-to-catch-it.aspx) because this tool can also help Microsoft Internet Security & Acceleration (ISA) administrators in some scenarios. Thank you for sharing this information.

—Yuri Diogenes,
Senior Security Support
Escalation Engineer,
Microsoft Corporation

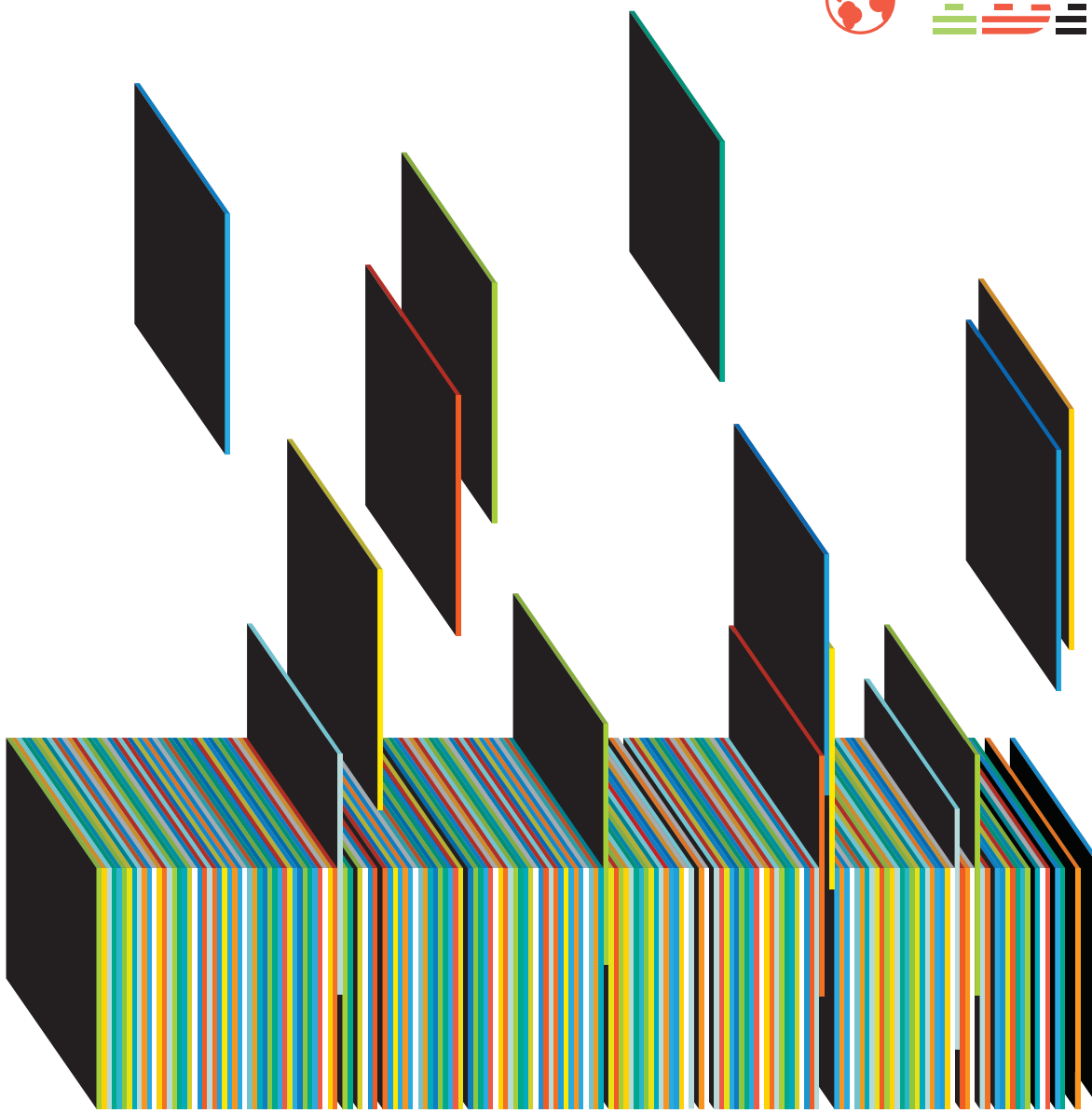
*Windows IT Pro* welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Smarter technology for a Smarter Planet:

# Building the extraordinary into everyday things.

By next year, the average car will require over 100 million lines of software code, and a commercial airplane, over 1 billion. It's approaching the point where a car or a plane isn't simply a car or a plane anymore. What makes them truly unique is the underlying software—the invisible thread—that infuses them with intelligence. In the past year alone, 66% of the products developed included embedded software. Today, software is a core strategic business asset. Unfortunately, 41% of software projects fail to deliver the expected ROI. Only IBM has the experience, the resources and the solutions to build more effective software design and delivery processes for the world's leading businesses.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/delivery



## Read on twitter

On a Windows Server 2008 R2 File Server Cluster we're seeing failover/failback times within two seconds. Nice! —@alsugano Wed, Sept 2, 2009

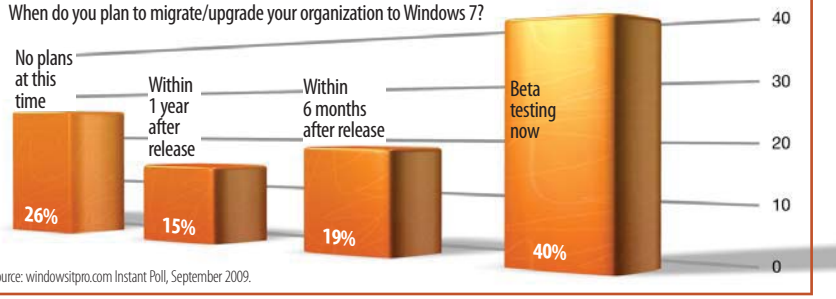
## Overheard

Proof that Steve Jobs is afraid of buttons:

1. Mac mice. 2. iPhone. 3. Turtlenecks.

**Instant Poll Results**

When do you plan to migrate/upgrade your organization to Windows 7?




Source: windowsitpro.com Instant Poll, September 2009.

# Windows 7: Migrate or Wait?

*from the Windows IT Pro Magazine Forum on* LinkedIn

**Q** Microsoft expects to release Windows 7 before the end of 2009. What are your migration plans? Will you move immediately on release? Wait 6 months? A year? If you do plan to move quickly, what is compelling you to do so? —Amy Eisenberg, Executive Editor, *Windows IT Pro*

*I'll be reviewing the compatibility of Windows 7 with my current legacy applications and the application vendors. We are currently an XP shop but do have the hardware in place to make the upgrade. So far, in our trials, it looks promising. More promising than Vista did when we initially tested it. —Chris Muncy*

*We will upgrade to Windows 7 on our next hardware refresh, which should be in 18–24 months. Hopefully we will have some 2008 R2 servers in place by that time to take advantage of Direct Access. —Peter Diamond*

*We are definitely upgrading. We will wait at least 6 months though. I am shooting for a summer 2010 roll out. We skipped Vista due to software compatibility issues, but so far, our testing has been positive with Windows 7. Our current hardware will support a large scale rollout of 7. Other than the time to do it, it should be fairly painless. (Famous last words :P)—Robert Jones*

**Q** Sounds like shops on XP don't have any major concerns about migrating to Windows 7, other than finding the time to get it done. Has the current economic climate affected your plans in terms of timing for your migration? —Amy Eisenberg

*Not for us. I work for a university and while there have been budget cutbacks, we haven't lost a crippling amount from IT. Plus, we have a site license for virtually all of Microsoft products so cost is not as big of an issue here. We do things on a semester basis. Since Windows 7 will be released during the fall semester, we will be using the spring semester to get our images and final software testing completed. If all goes well, we should be able to push it out in August of 2010 for use by returning and new students in the fall of 2010. We do have a plan B, but I hope we don't need it. —Robert Jones*

*The key to migration is legacy applications that cannot be replaced or upgraded due to the economic situation. If the legacy applications work correctly as new machines are deployed, we may leave Windows 7 on them and phase it in. If legacy applications prove to be a problem we will buy Win7 licenses and continue with WinXP until we can afford to replace or rewrite the applications that don't work. —Mike Johnson*

*Dell made an anouncement yesterday that they started releasing Win7 drivers last Friday. I have a 2 year old Latitude laptop that I just wiped, installed 32 bit Vista, then upgraded to Win7. Wow.... Painless and everything came up.—Chris Muncy*

*I have been running Windows 7 for a little over a week now on a Dell Latitude D630, 64-bit version. It was a breeze to upgrade and I have [not] had to load a single driver. All of my apps work and it's faster than Vista x64.—Robert Jones*

# Thinking outside the box depends on what's in the box.

Energy demands in today's server rooms aren't simply a matter of costs. They're increasingly impacting day-to-day operations. A recent study found that an estimated half of all businesses have experienced IT outages due to power and cooling issues.[1] The entire architecture of the IBM BladeCenter® HS22 is designed to give you greater efficiency at every level—from its highly efficient design and Intel® Xeon® Processor 5500 Series to its advanced management software, such as IBM Systems Director, which actively monitors power consumption, to built-in sensors that optimize cooling. All of which can add up to 93% in energy savings over the previous generation of rack servers. Learn how you can see a return on your investment in as little as three months[2] at ibm.com/hs22

Systems, software and services for a greener planet.

IBM®



intel® Xeon® inside™

Powerful. Intelligent.

[1] Source: IDC Market Analysis #215870, Volume 1, December 2008, Worldwide Server Energy Expense 2008–2012 Forecast. [2] Return on investment and power savings calculation based on 11:1 consolidation ratio scenario of 166 Intel 1U 2 socket servers to 14 BladeCenter HS22 servers and savings in energy costs, software license fees and other operating costs. Actual costs and savings will vary depending on individual customer configurations and environment. For more information, visit www.ibm.com/smarterplanet/claims. 

# Thurrott

"Microsoft finally has a credible alternative to the virtualization market leader, built on top of the Windows Server platform you already know."

# What You Need to Know About Hyper-V 2.0

With the release of Windows Server 2008 R2 this fall, Microsoft is ushering in a surprisingly comprehensive update to its core Windows Server product. But no Windows Server technology is arguably as central to the software giant's strategy as the Hyper-V hypervisor-based virtualization platform, which has gotten a major makeover in its 2.0 release. Here's what you need to know about Hyper-V 2.0.

## Hyper-V 2.0 High-Level View

Hyper-V 2.0 is available as an installable role in Server 2008 R2 Standard, Enterprise, and Datacenter Editions. It's also available in the midmarket-oriented Server 2008 R2 Foundation Edition and as a free, bare-metal standalone server called Microsoft Hyper-V Server 2008 R2. All of these products are available only in 64-bit versions.

Hyper-V is a hypervisor-based server virtualization platform. It provides the ability to run virtualized client and server guest OSs under the host Server 2008 R2 OS (or, in the case of Microsoft Hyper-V Server 2008 R2, under that basic host OS), and forms a virtualized infrastructure where you can consolidate older servers, deploy and manage new server installations, and perform other tasks traditionally associated with physical machines. Hyper-V 2.0 has been streamlined to run effectively in a variety of environments, from small-to-midsized businesses (SMBs) to the largest data centers.

## What's New in Hyper-V 2.0

Live Migration is arguably the signature new feature in Hyper-V, and it significantly closes the gap between this solution and VMware's more mature virtualization products. Live Migration provides a way to move a running virtual machine (VM) from one physical host server to another in near real-time, with no service interruption to connected clients.

Hyper-V 2.0's Live Migration functionality works with another new feature of the underlying Server 2008 R2 platform, Cluster Shared Volumes, to provide failover capabilities as well. Each server must exist within the same failover cluster and access the same shared storage.

From a scalability perspective, Hyper-V supports heady resource allotments, and with this release, the bare-metal Microsoft Hyper-V Server 2008 R2 product corresponds to the specifications of the broader Server 2008 R2 platform (whereas the first version was far more constrained). It supports up to eight physical processor sockets (64 for Datacenter Edition), up from four. Processor core support is also up dramatically, to 64. The original shipping version of Hyper-V supported 16 processor cores, though that was later increased to 24 via a software update. The maximum number of virtual processors is eight times the number of logical processors (essentially equivalent to the number of physical processor cores).

Additionally, Hyper-V 2.0 supports up to 1TB of RAM and up to 16 cluster nodes. The maximum number of running VM guests is 384, up from 192 in Hyper-V 1.0.

Hyper-V 2.0 also improves virtual networking performance via several new networking advances, including VM Chimney, which provides TCP offloading functionality that maps virtual network traffic to a specific physical NIC. And the Jumbo Frames feature that was introduced in Server 2008 is available to VMs as well, improving network throughput and reducing CPU utilization.

## The Standalone vs. the Installable Role

Although Hyper-V 2.0 in free, standalone Microsoft Hyper-V Server 2008 R2 is largely identical to that in the mainstream Server 2008 R2 editions, it's also different. Microsoft Hyper-V Server 2008 R2 supports clustering, for example, but doesn't include any virtualization rights for guest VMs. (Server 2008 R2 Enterprise Edition comes with four VM licenses, while Datacenter Edition includes unlimited VM licenses.)

For admins, the biggest difference is that Microsoft Hyper-V Server 2008 doesn't include a local administration console. Instead, this free server provides a simple command-line–based tool for making simple configuration changes only (i.e., setting the machine name and joining a domain). To manage Microsoft Hyper-V Server 2008 R2, you need to do so remotely using Microsoft Remote Server Administration Tools (RSAT) in Server 2008, Server 2008 R2, or Windows 7. (For the latter, a separate download is required.) Or you can use System Center Virtual Machine Manager 2008 R2.

## Recommendation

From a performance and scalability perspective, Hyper-V 2.0 makes upgrading a no-brainer for existing customers. But the product is particularly compelling for new customers as well.

Though it's free, Microsoft Hyper-V Server 2008 R2 is now largely equal to the functional capabilities of its more expensive siblings, and it's the perfect way to get your feet wet with virtualization. Hyper-V 2.0 is nearly as mature and full-featured as VMware's solutions. With Hyper-V 2.0, Microsoft finally has a credible alternative to the virtualization market leader, and it's built on top of the Windows Server platform you already know and trust.

InstantDoc ID 102764

**PAUL THURROTT** (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Smarter technology for a Smarter Planet:

# Service in the age of smart assets.

Smart assets are making it possible to spread intelligence into everything from power lines to railroad lines to assembly lines. The challenge is: how do you choreograph the physical and the digital to provide the quality services your customers expect and the flexibility your business needs? IBM's approach to service management can help you extend visibility, control and automation through all of your company's services so you can easily modify existing services or quickly add new ones, laying the groundwork for a more dynamic infrastructure. We're helping companies all over the world—20 of the 20 top telcos and 7 of the 10 largest automotive manufacturers—reach beyond the datacenter to deliver flexible services in a smarter way.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/svcmgmt

# Minasi

"Sometimes Set just won't satisfy certain needs—that's when you need to graduate to the more capable Setx."

# Enhanced Environment Variable Control with Setx

## It's the tool you need when Set doesn't do the trick

Last month, I covered some intriguing capabilities of the essential Set command (in Windows 2000 and later)—namely, convenient methods for soliciting user input to a batch file and performing arithmetic on environment variables. But what about getting data into an environment variable in the first place? That speaks to the command's more basic uses. And in that regard, sometimes Set just won't satisfy certain needs—that's when you need to graduate to the more capable Setx.

Many batch files that utilize an environment variable set its value either with a solicitation for user input (as I showed you last month with the /p switch) or with a simple Set command:

```
set myname=Mark
```

That command works fine, but sometimes you need to stuff other kinds of things into an environment variable, such as the result from a command (e.g., extracting the round-trip time from a Ping statement) or a value in a registry entry.

For at least 10 years, a resource kit tool called Setx has let you do that, and in Windows Vista and later, Setx is built into the OS. As you'll see, Setx can be a bit quirky (no surprise to fans of resource kit tools), but it can also provide the basis for some powerful batch files.

Suppose, for example, that you want to grab a registry value and put it into an environment variable. You need to retrieve the name of the organization that your copy of Windows is registered to, either for a report or to verify that the organization in the registry is the correct one. Windows stores that information in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization registry subkey. With the command

```
setx regorg /k "HKLM\SOFTWARE\Microsoft\Windows NT\
  CurrentVersion\RegisteredOrganization"
```

Setx will extract the value and put it into an environment variable. Setx can grab data from a number of sources—not just the registry—but in this case, the /k option directs Setx to the registry. At first glance, the string in quotes looks like a registry subkey, but it isn't: It combines the name of a registry subkey and the name of the value entry inside that subkey whose contents you want Setx to store in an environment variable named *regorg*. If all goes well, Setx's output looks like

```
Extracted value: "MR&D".
SUCCESS: Specified value was saved.
```

Setx doesn't have an option to suppress this wordy output, but you could always block the Setx chatter from appearing onscreen by redirecting the output to the nul device:

```
setx regorg /k "HKLM\SOFTWARE\Microsoft\Windows NT\
  CurrentVersion\RegisteredOrganization" >nul
```

So, now you have an environment variable named *regorg* in the system. However, remember that "quirk" I mentioned? For reasons only Setx's developers know, Setx creates that environment variable and populates it—but it doesn't communicate the situation to the copy of the environment variable in your current command-line window. Therefore, any command that you run in the command-line window where you just ran the Setx command won't be able to see the value that you just created in the environment variable. For example, typing *set regorg* would yield the error message *Environment variable regorg not defined*. To see the new environment variable value, you'd need to open a second command window and run your command.

Techies who use environment variables know that Windows stores some of them in the system's profile and some in the user's profile. Typing *set* from a command prompt shows environment variables from both the system and user profiles, with no indication of any given environment variable's source. To my knowledge, there's no way to use the Set command to see only the system-related environment variables or the user-related environment variables, although you *can* see the difference by clicking the Environment Variables button on the Advanced tab of your computer's System Properties page. With Setx's /m option, you get a little more control over environment variables that you create. When you use the /m option, your new environment variable goes into the system profile rather than your user profile.

If you're writing in-depth batch files, Setx can help you, so it's good news that it's "in the box" in recent Windows editions. Next month, I'll show you what else it can accomplish.

InstantDoc ID 102706

**MARK MINASI** (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro,* an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

**Otey**

"You can manage your entire virtualization infrastructure with VMM, including both Microsoft Hyper-V and VMware ESX Server virtual machines."

# New Features in Virtual Machine Manager 2008 R2

## Live Migrations, improved storage features, and broader management options bolster VMM

Of all the different technologies at Microsoft, there's no doubt that none is evolving faster than System Center Virtual Machine Manager (VMM). You can manage your entire virtualization infrastructure with VMM, including both Microsoft Hyper-V and VMware ESX Server virtual machines (VMs). You can also create and deploy new VMs as well a manage VM states and storage. The new VMM 2008 R2 release is designed to take full advantage of the recent Windows Server 2008 R2 and Hyper-V R2 improvements. Here are the top ten new features in VMM 2008 R2.

1 **Live Migration**—Without a doubt, the most important new feature in VMM 2008 R2 is Live Migration. This feature is the equivalent of VMware's VMotion; it lets you move a virtual machine (VM) between Hyper-V hosts with no downtime. Live Migration requires Windows Server 2008 R2 or Hyper-V Server 2008 R2.

2 **Support for the Clustered Shared Volume (CSV) file system**—To support Live Migration, Microsoft added the CSV file system to Server 2008 R2. CSV lets multiple hosts in a cluster simultaneously access a shared LUN. The CSV feature also facilitates easier storage management by letting you store multiple VM files on the same LUN.

3 **Support for hot add/removal of storage**—VMM 2008 R2 supports the hot addition and removal of storage on Hyper-V VMs. This new feature lets you add Virtual Hard Disks (VHDs) to running VMs and remove VHDs from running VMs with no downtime.

4 **Rapid provisioning**—The new rapid provisioning feature lets administrators utilize underlying SAN technologies for cloning VM files, then combines the cloned image with the ability to supply a VMM template for customizing the guest OS. Rapid provisioning doesn't have a UI. Instead, it's driven by PowerShell commands.

5 **Quick Storage Migration**—VMM 2008 R2's Quick Storage Migration lets you move Hyper-V VM storage between different LUNs with minimal downtime. Quick Storage Migration is particularly useful for taking advantage of CSV storage and consolidating your VM files on a shared LUN. Quick Storage Migration requires between 20 seconds and a couple of minutes of downtime, depending on the size of your VMs and the performance of your storage subsystem.

6 **Support for VMware Storage VMotion**—Closely related to Quick Storage Migration is support for VMware Storage VMotion. Storage VMotion lets you move an ESX Server's VM files between LUNs with no downtime. Like VMM 2008's support for VMotion, support for Storage VMotion requires VMware vCenter Server.

7 **Support for Veritas Volume Manager**—Another new storage-related enhancement in VMM 2008 R2 is built-in support for Veritas Volume Manager. VMM 2008 R2 recognizes Veritas Volume Manager disks as a cluster disk resource.

8 **Enhanced iSCSI SAN support**—VMM 2008's support for iSCSI SANs has been improved so that multiple LUNs can be bound to each iSCSI target. This capability provides broader industry support for more iSCSI SAN hardware options.

9 **Maintenance mode**—Maintenance mode lets you specify that you're going to perform some type of hardware or OS maintenance to a Hyper-V host. When you use maintenance mode on a Hyper-V host, all the VMs that are Live Migration–enabled are migrated to another host. VMs that aren't configured for Live Migration automatically have their state saved.

10 **Host compatibility checks**—One of the limitations of moving VMs between hosts is the fact that the hosts must have compatible processors. For example, you can't move a VM from a Hyper-V host that uses an Intel CPU to a Hyper-V host that uses an AMD CPU. VMM 2008 R2's host compatibility checks verify that the CPUs of different hosts are compatible for actions such as Live Migration and Quick Storage Migration.

InstantDoc ID 102752

**MICHAEL OTEY** (motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

# What if fragmentation never happened?

Even a good defragmenter working invisibly in the background can't touch a specific *hidden source of performance loss* caused by fragmentation that many IT managers are unaware of. Many know that all systems suffer from fragmentation and that fragmentation bottlenecks the slowest component on every computer: the hard drive. Automatic defragmentation catches fragments soon after they are created and returns files to a contiguous state. It's a reactive fix.
*But what if fragmentation never happened?*

Today's network efficiencies depend on achieving greater throughput. If it's bottlenecked, it doesn't much matter how much whiz-bang you threw money at in the way of equipment, your productivity suffers. The ability of a server, workstation or laptop to generate high I/Os per second (IOPS) has become one of the key throughput abilities system managers look for when upgrading their networks. I/Os are a critical resource and the more effectively they are employed toward direct production, the more work gets done in the least amount of time.

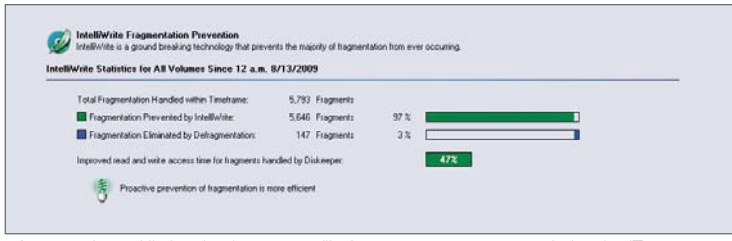
## The real damage

When fragmentation occurs, the system has already wasted precious I/O resources by writing files into fragments of space on the disk. This cuts into the system's "effective IOPS": system activity that leads directly to a desired product, not a preparatory activity needed so productivity can occur. This event has tremendous ramifications. As a simplified example, if you need 1500 IOPS to get a job done in the afforded period of time and your system will only give you 1000, you must either buy more hardware to get that productivity, do less work, or wait. The more I/Os that occur, the more disk head movement, the more energy the site consumes and the more cooling is required.

The problem worsens with scale. The busier a system or a network is, the more fragmentation is being created by "diverted" split I/Os and the more overexpansion and provisioning is needed to get a job done.

## Introducing Diskeeper® 2010 performance technology with IntelliWrite™ — the first ever fragmentation prevention technology.

Diskeeper Corporation, the inventors of automatic defragmentation, has just released a technology that takes system performance and efficiency to a previously unattainable level. IntelliWrite file prevention technology proactively prevents up to 85% and more of the fragmentation a system can generate. This technology is completely new and no other solution comes close to the benefit IntelliWrite can have on every Windows® network. IntelliWrite keeps disks clean and fast by intelligently writing contiguous files to the disk.




*An at-a-glance UI showing how many file fragments were prevented give the IT manager an important window on system speed and efficiency gains.*

So, what if fragmentation never happened? Benefits like these would become commonplace:

- More productivity with the safi e hardware
- Longer cofi puter life
- Cofi pletely new levels of speed and efficiency
- Significantly less energy consufi ption including cooling requirements
- Faster file reads and writes
- Minifi ized/elifi inated data replication traffic and storage requirements.

## You can have all this with new Diskeeper 2010. Get more information here:

**www.diskeeper.com/2010**



Diskeeper 2010

The only way to prevent fragmentation ***before*** it happens.™

# Mangipano

"When no information is output to the system about a problem, you can use the debugger to identify what's going on in the process."

# Further Adventures in Debugging

## 5 tips for tracing the source of problems by using the Windows debugger

How many times have you faced a problem where no error information was displayed on screen and related logs provided no data to help trace the failure? To help you solve such problems, I'll provide some tips that admins who are new to debugging can use as a starting point. I'll demonstrate these tips by using an application that I support—Device Manager—which you're probably familiar with. I'll spare you the mind-numbing walkthrough of the entire assembly-level debug of this particular problem and instead offer some basic debugging techniques to help you as you cross over into the intangible binary world of debugging.

### Tip 1: Open a process in the debugger.

When no information is output to the system about a problem, you can use the debugger (windbg.exe) to identify what's going on in the process. (For more information about getting started using the debugger, see "Administrators' Intro to Debugging," June 2009, InstantDoc ID 101818.) Before launching a process in the debugger, you'll need to obtain the command line to type into windbg to launch that process. You can find the command line by using Process Explorer (technet.microsoft.com/en-us/sysinternals/bb896653.aspx); to obtain the command line, simply double-click the process, and you'll see the command line displayed on the Image tab.

After opening the Windows debugger from the Debugging Tools for Windows Start menu group, you can launch Device Manager by selecting Open Executable from the File menu. Enter the command line that you'd normally use to start the process.

### Tip 2: Find out as much as you can before debugging.

Before jumping into the debugger, get some basic information about the code you want to study. Determining where to start debugging often begins outside the debugger. You need a way to determine the names of functions related to your problem. For example, if your application is reporting an error stating it was unable to open a registry key, your goal is to identify the function that's used to open registry keys. So how do you know what functions are used for different tasks? Although the function names provide some clues, you can use MSDN to research what calls are available. For example, a quick MSDN search on "registry functions" would locate the MSDN documentation listing these functions at msdn.microsoft.com/en-us/library/ms724875(VS.85).aspx. You'd see that RegOpenKeyEx is the function used to open registry keys.

You can use the free Dependency Walker tool (depends.exe), available at www.dependencywalker.com, to obtain information about relevant functions. Dependency Walker displays what DLLs a binary uses and the function names that the binary uses from the DLL. Obtaining this information is easy: Launch depends.exe, then open the binary file that you're troubleshooting via the open command from the File menu. Dependency Walker will then display the names of the functions that this application calls when it executes. This information is important to your debugging because it lets you identify interesting calls that may be related to the problem. For example, if your application is popping up a message stating that the network connection attempt failed, you'd search Dependency Walker's output for function names that appear related to opening network connections. You can then use the debugger to investigate these calls as they're made.

As an example, let's use Dependency Walker to open devmgr.dll. This is the binary comprising the code that mmc.exe uses to create the Device Manager snap-in. As you can see in Figure 1, Dependency Walker shows that devmgr.dll imports various functions related to device enumeration from setupapi.dll. In case you're

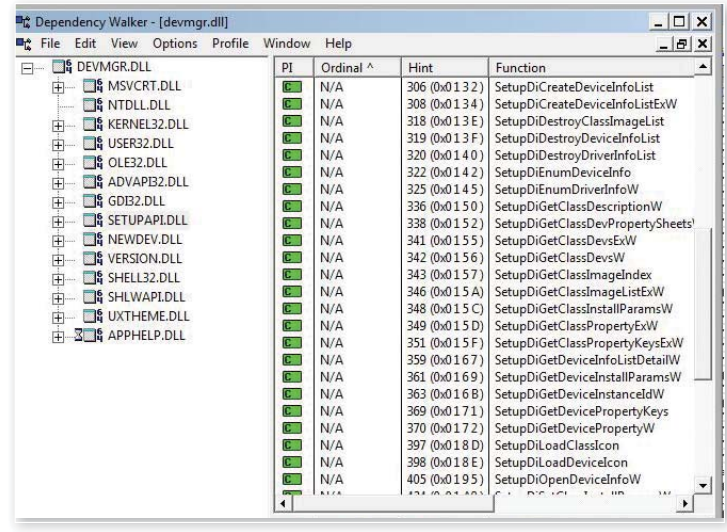



Figure 1: Viewing devmgr.dll–related functions in Dependency Walker

```
0:000> x devmgr!*Devices*
72af71a9 devmgr!CMachine::CreateClassesAndDevices = <no type information>
72aef942 devmgr!CClass::GetNumberOfDevices = <no type information>
72af0810 devmgr!ViewDevicesMenuItems = <no type information>
72af65fd devmgr!CMachine::DestroyClassesAndDevices = <no type information>
```

Figure 2: Using the x debugger command

```
0:000> wt -l2
Tracing setupapi!PNP_GetDeviceList to return address 770edf88
   10     0 [  0]    setupapi!PNP_GetDeviceList
    1     0 [  1]              setupapi!NdrClientCall2
    3     0 [  1]                    rpcrt4!NdrClientCall2
<Omitting lengthy output>
```

Figure 3: wt command output

wondering how I determined that devmgr.dll is the DLL used to create Device Manager, devmgmt.msc is actually an XML file that lists devmgr.dll in the text. You can use Notepad to open it.

## Tip 3: Set breakpoints.

Once you start a process in the debugger, the debugger will stop at an initial breakpoint during process initialization. However, this isn't usually the best place to start debugging. Execution of a program typically consists of many different assembly instructions and function calls. However, only a small number of these may be related to the problem at hand. You need a way to get the debugger to allow the program to run until the functions that you've identified as relevant (by using depends.exe) are encountered. To accomplish this, you set breakpoints.

You can set a breakpoint against a function by using the bp (set breakpoint) command. Then you use the g (go) command to resume execution of the threads in the process so that they can continue running until something causes the debugger to break-in again. Here are the commands and output:

```
0:000> bp setupapi!CM_Get_Device_ID_
  List_ExW
0:000> g
Breakpoint 0 hit
```

When this breakpoint is hit, you'll be at the beginning of the function call that you're interested in. In tips 4 and 5, we'll review some commands you can run once you get to these locations.

In the previous output, the debugger informed us that we've hit breakpoint zero. You can list the breakpoints by using the bl (breakpoint list) command. We have only one breakpoint, which is numbered as zero.

```
0:000> bl
0 e 770edf2d

0001 (0001)

0:****
setupapi!CM_Get_
Device_ID_List_
  ExW
```

So how can you search for the names of the functions that you might want to set breakpoints against? The x (examine symbols) command can use the symbol information to obtain functions and other data matching a wildcard pattern. The example in Figure 2 lists all symbol data matching the wildcard pattern *Devices* from the devmgr module. You can then set breakpoints against any of these functions.

If devmgr.dll hasn't yet been loaded into the process, this command will fail. In such situations, you'll need to instruct the debugger to halt when a specific module is loaded. The following command will cause the debugger to break-in when setupapi.dll is loaded:

```
0:000> sxe ld:setupapi
0:000> g
ModLoad: 770e0000 771e8000   c:\
  windows\system32\setupapi.dll
```

## Tip 4: Identify call flow.

Once you've hit your breakpoint, you can find out what called the function and what the function calls (i.e., call flow) by examining the stack using the kC (display stack back trace) command. In our example, I ran the kC command after hitting a breakpoint that I had set against setupapi!PNP_GetDeviceList. Stacks grow upward. This means that the top-listed function was the last one called. The kC command output will show the stack after hitting a breakpoint set against setupapi!PNP_GetDeviceList. Devmgr.dll has called into setupapi.dll to enumerate the list of devices.

To identify the calls a function makes by watching and logging its execution, you can use one of the most powerful commands in the Windows debugger: wt (watch trace). You can run this command from the beginning of a function call; doing so will output the calls made by this function to the screen. In the example in Figure 3, I used the -l2 parameter to limit the output depth to two levels. In this example, setupapi!PNP_GetDeviceList called setupapi!NdrClientCall2, which then called rpcrt4!NdrClientCall2.

## Tip 5: Identify whether a function call returned an error.

Once you hit a breakpoint that you set for a function, how do you identify whether these functions have returned an error code? You use the gu (go up) command to return from the function, then use the r command to examine the return value.

The gu command resumes execution until the current function returns. In this case, the gu command runs the PNP_GetDeviceList function, then stops breaks-in immediately when the function is done. The r (register) command outputs the contents of registers. $retreg represents the return register, which can be used to identify whether a function has finished successfully or returned an error. We received an error 0x1d from PNP_GetDeviceList(). I located the return value for PNP_GetDeviceList documented at msdn.microsoft.com/en-us/library/cc239018(PROT.10).aspx: *An error occurred during an attempt to read the registry.*

## Final Steps

The device manager issue was resolved by using the p (step) command to trace through the execution of the function. The debug trace session showed that setupapi!PNP_GetDeviceList had made an RPC call directed to interface 8d9f4e40-a03d-11ce-8f69-08003e30051b. With a little help from Process Monitor, I found that this RPC call was answered by the function umpnpmgr.dll!PNP_GetDeviceList(), which was running in the services.exe process. This call had failed with NAME_NOT_FOUND because of registry corruption. I rebooted using the Last Known Good registry configuration. Problem solved!

InstantDoc ID 102867

**RYAN MANGIPANO** is an escalation engineer on Microsoft's Global Escalation Services team in Las Colinas, Texas. He specializes in core Windows troubleshooting and advanced debugging. For information about Windows debugging, visit blogs.msdn.com/ntdebugging.


*APC Back-UPS ES 750G is the energy-conscious choice. Save up to $40 per year* on your electric bill.*

**SmartShedding® Technology**

Allows the master outlet to sense when your computer has either been turned off or gone into sleep mode, so it can shut off power to peripherals plugged into the controlled outlets–saving you power and money.

# Enviably Green.

## Uses up to 5x less power in normal operation than any other battery backup.

### Let's protect what's important.

What's in your computer? Photos, music, personal files, financial data, broadband access, videos, and more. Your computer has never been more important, and yet it has never been at higher risk for damaging power surges and other disturbances.

So like most people, you need to protect your assets. But like most people, you'd also like to protect the environment. With our new energy-conscious products, you can do both. Energy efficient by design, our new smart products protect the power going into your computer, at a cost that is quickly offset by big energy savings. How? Not only do the new Back-UPS ES and SurgeArrest use power wisely, they also boast a master/controlled outlets feature that automatically powers down idle devices to conserve energy.

**APC power protection products are available at:**

BEST BUY · CDW · STAPLES that was easy: · PC Connection

*"The price tag on the new UPS is $99. While I'm not in the habit of endorsing products in this blog, if you're in the market for a workstation-class UPS, why not opt for the greener option?"*

*– Heather Clancy, ZDNet.com*

In fact, while protecting your power supply, we're up to five times more energy efficient than any other solution. By saving you $40 a year in energy costs, our Back-UPS ES pays for itself in two short years. The high frequency, low copper design has a smaller transformer and environmental footprint. Even the packaging has been carefully selected and manufactured to maximize use of recycled materials and minimize waste.

In this world, every decision you make counts. So protect your power with a battery backup that works to protect the environment. It conserves power, pays for itself, and is backed by APC's 20-plus years of Legendary Reliability. For more information on this or our other great products, or for information about environmentally responsible disposal of your old battery, visit ***www.apc.com***

## Energy-efficient solutions for every level of protection:

Save $25 per year* on your electric bill!

### Surge Protection

Starting at $34

Guaranteed protection from surges, spikes, and lightning.

7 outlets, phone/fax/modem protection, master/controlled outlets

SurgeArrest P7GT

Save $40 per year* on your electric bill!

### Battery Back-UPS

Starting at $99

Our most energy-efficient backup for home computers.

10 outlets, DSL and coax protection, master/controlled outlets, high frequency design, 70 minutes of runtime†

Back-UPS ES 750G

*APC can help with your other power-protection needs. Visit www.apc.com to see our complete line of innovative products.*

## Enter to Win a Back-UPS ES 750G! (A $99 value)

*Also, enter key code to view other special offers and discounts.*

Visit www.apc.com/promo Key Code m777w or Call 888-289-APCC x8245 or Fax 401-788-2797

APC® Legendary Reliability®



*Average savings are based on comparable competitive models, and are comprised of two energy-saving features: an ultra-efficient electrical design, and the master/controlled outlets feature. †Runtimes may vary depending on load.

# DEEP DIVE INTO VMware vSphere eLearning Series with John Savill

## WHEN
December 10, 2009

## WHERE
Your computer

## COST
$99 for all 3 lessons

## LESSONS
**11:00 am ET** – VMware Virtualization Capabilities and the vSphere Platform

**12:30 pm ET** – Deploying and Managing vSphere

**2:00 pm ET** – High Availability and Resource Management with vSphere

## HOW
Register at www.windowsitpro.com/go/elearning/VMwarevSphere

## Explore the major functionality capabilities of the vSphere virtualization platform, including identification of the changes from ESX 3.5.

Join MVP John Savill on December 10, 2009 for 3 in-depth lessons and Q&A sessions on how to ensure that vSphere is deployed and maintained in the most optimal way.

What you'll take-away from this exclusive eLearning series:

- Understanding the different types of virtualization available and how they are best suited to your organization
- Understanding how vSphere is deployed and managed with focus on additional capabilities through Virtual Center
- Learning about the high availability capabilities of vSphere through vMotion and storage migration capabilities, including disaster recovery site capabilities

## INSTRUCTOR:

John Savill is the author of the popular FAQ for Windows and a contributing editor to Windows IT Pro. He is an advisory architect for EMC's Microsoft consulting practice. He's an MCITP: Enterprise Administrator for Windows Server 2008 and a 10-time MVP. His latest book is The Complete Guide to Windows Server 2008 (Addison-Wesley).

Learn more about the speaker, lessons, and how to reserve your seat at:
www.windowsitpro.com/go/elearning/VMwarevSphere

Windows IT Pro

# TOOL TIME

windowsitpro.com

- WinDirStat
- Active Directory
- Dnscmd

## WinDirStat Simplifies Finding Where Your Disk Space Is Going

When I need to find out why a hard drive is running out of free space, simply searching for files by size using Windows' built-in search capabilities isn't always up to the task. I can certainly find the largest files on a drive, but they lack the context of surrounding files and file types. Furthermore, you can't identify problems caused by large numbers of smaller files. Instead, I prefer to use the free WinDirStat directory statistics tool (windirstat.info). Inspired by the KDE tool KDirStat, WinDirStat is a portable application that provides multiple views of file-space usage. It's compatible with Windows 95 and later.

The multiple usage views simplify getting a quick overview of disk usage. An expandable folder listing shows folder usage sorted by size, including percentage of space used, absolute size, and number of items. An extension listing provides a breakdown on usage by extension and provides a color key for the file types that are displayed in the Treemap view.

The Treemap view is what I use to quickly get a usage overview. Blocks, proportional to size, represent files and are arranged so that each larger rectangular grouping is a directory or subdirectory. With a few seconds of inspection in WinDirStat, I usually know why a drive is getting full.

One caveat to keep in mind is that on Windows 7 and Windows Vista, WinDirStat's uninstaller doesn't correctly remove the All Users\Start Menu\Programs folder for WinDirStat or the installing user's desktop shortcut. You'll have to remove these leftover pieces yourself. However, WinDirStat doesn't actually need the installation routine, so you can just install it once and copy WinDirStat .exe and WinDirStat.chm to a network location or USB drive for mobile use.

—Alex K. Angelopoulos, IT consultant

InstantDoc ID 102794

# READER TO READER

## Protect AD from Administrative Errors

Imagine that you're the enterprise administrator of a multidomain Active Directory (AD) environment. You're attending a presentation by your new CIO Steve Johanson justifying the sizable IT budget to the shareholders. The meeting is supposed to start in 5 minutes and your CIO can't access his presentation on the company SAN. When you look up his account to make sure he has the necessary access permissions, you find that his account is missing. You look at the change log and see that your junior administrator was supposed to remove the account for Steve Johnson, who just retired. Then it dawns on you—the wrong user was removed. Now it's panic time. Fortunately, the CIO knows a few good jokes and can entertain the shareholders while you reanimate his user account, give him a new password, and add him back to all the groups in the other domains so he can access the presentation as well as the rest of his reference material. Fortunately, the CIO understands that mistakes happen, but you wish it could all have been avoided.

Most administrators have been in situations in which a mistake has led to users being accidentally deleted, removed from groups, or granted access they shouldn't have. Although you can purchase expensive AD backup utilities or set up complicated scripts that let you recover an account in only a few minutes, wouldn't it be great if you could avoid these types of mistakes all together?

Protecting AD objects from administrative errors is challenging. One way to meet this challenge is to have administrators check each other's changes before implementing them. Another way is to use third-party tools to automate changes. One solution that not many people are aware of is to use selective authentication, which was introduced in Windows Server 2003, in an external trust.

The selective authentication solution takes some work to set up initially, but it provides an effective way to audit AD changes. When selective authentication is enabled, users (in this case, administrators) in a trusted domain are explicitly granted rights on specific computers in the trusting domain, so you can control what resources they can access.

Here's how to set up an AD environment for selective authentication:

1. On the production side of the AD forest, set up a lag site that contains one domain controller (DC) but no associated subnets. Set up a strict replication schedule in which you either allow replication at very limited times or require all replication to be manually triggered. (Turning off all scheduled replication on a site link will generate spanning tree error events on other DCs.) The replication limitation is controlled through the site link schedule.
2. Set up a second forest (aka the Admin Forest) that contains two or more DCs for redundancy. Place all the administrator accounts for which you want to validate changes in this forest.
3. Set up an external trust between the two forests. Although the trust can be domain based or forest based, you need to set it up as a one-way trust, where the outgoing or trusted domain is the admin domain and the trusting side is the production AD. Instead of using the default authentication method, choose the selective authentication method.
4. Grant authentication permission.

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.

*If we print your submission, you'll get $100.*

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the InstantDoc ID text box.

You now have a group of administrator accounts in the Admin Forest that can see the trust to the production forest but can't authenticate to any of the resources in it. So, you need to grant the *Allowed to Authenticate* permission to the administrator group on the DC in the lag site (aka lag DC).

James R. Day

5. Grant activity rights. Go through your standard delegation procedure to grant the administrators the rights they need to perform their jobs, such as adding or deleting objects, modifying DNS properties, and creating Group Policy Objects (GPOs).

Selective authentication combined with the *Allowed to Authenticate* permission on a single DC forces all changes to happen only on that machine. With this setup, administrators can perform their duties, but any mistakes are restricted to one DC in a site that doesn't perform any user authentication. The changes remain there until the replication schedule permits them to propagate. If the replication schedule is manual (i.e., no scheduled times for replication), the changes won't propagate until somebody manually releases them.

This brings us to how to use this solution. You should separate your administrators into two groups. The administrators in one group make changes on the lag DC. The administrators in the other group regularly look at all the changes that have been made on the lag DC. If the changes are acceptable, they force a replication into the live environment. If the changes aren't valid, contain mistakes, or violate company policy, they inform the administrator who made the changes so that he or she can remedy the situation.

So, how does a verification administrator check the changes? In Windows 2003 and earlier, the easiest way is to have Audit DS Changes enabled in the DC's audit policy. This allows all changes made on the DC to be recorded in the security log. Because all changes are being made on a single DC, the verification administrator just has to look at one log and search for any change events that have occurred since the last replication.

Windows Server 2008 introduced some better tools for reviewing directory service changes, such as Dsmain. With this tool, you can mount an LDAP database created in a backup (or created using the Ntdsutil utility), then use a script to compare all objects between the offline LDAP backup and the live lag-site forest, thereby letting you see all changes that have yet to propagate. Server 2008 also has enhanced event auditing, which lets you see more information about changes and create custom views to show only changed objects.

There are also third-party audit tools that you can use. These tools let you capture changes in real time and compare different databases on different DCs, providing an easy way to see what has changed.

Had the selective authentication solution been in place, the opening scenario would have played out differently. Here's what would have happened: The junior administrator sees he needs to delete the account for Steve Johnson, so he logs on to the Microsoft Management Console (MMC) Active Directory Users and Computers (ADUC) console in the Admin Forest using his account, which is also in the Admin Forest. He navigates to the production forest and tries to connect to a DC. Because selective authentication is being used in an external trust, he can only connect to the lag DC—all other DCs give him an access denied message. He searches for *Steve Joh** and accidentally deletes Steve Johanson on the lag DC. At this point, the mistake is made, but it's confined to the lag DC.

The verification administrator logs on to the production forest and looks at the changes made on the lag DC. He notices that the account for CIO Steve Johanson has been deleted. Instead of replicating the change to another site and allowing it to spread throughout the forest, he simply contacts the junior administrator about the problem. He also takes the lag DC offline until after the CIO's meeting is over. The CIO can access his resources and won't know about the mistake until he sees the monthly status report—at which point he will thank you profusely.

Note that there are a few caveats when using this solution:

- The chances of an erroneous DS change impacting the production environment have been mitigated but not eliminated. A verification administrator might miss seeing a problem and propagate an erroneous change. This is especially likely if there are a large volume of changes being made. Verification administrators can get caught up in the number of events and not look at them as closely as they should.
- The domain and enterprise administrator accounts still exist in the production forest and can make changes. So, if they really want to, administrators could circumvent the system and make changes directly on any DC in the production forest instead of on the lag DC.

Although these caveats exist, they're offset by the solution's potential benefits. Besides the obvious one (i.e., reducing the chance that an erroneous change impacts the production environment), the benefits include the following:

- You have a straightforward way to audit and report on heritage object changes (especially if you use Server 2008) because every change takes place on one DC.
- You add a bit of protection against account compromise. If an administrator account is compromised, the scope is restricted to the lag DC. So, all you need to do is wipe the lag DC and Admin For-

Had the selective authentication solution been in place, the opening scenario would have played out differently.

```
[/DP <FQDN>] -- fully qualified domain name of directory partition
                where zone should be stored; or use one of:
                  /DP /domain - domain directory partition
                  /DP /forest - forest directory partition
                  /DP /legacy - legacy directory partition
```

Figure 1: The Help information for Dnscmd's /dp switch

Rick Sheikh

est DCs clean, which is much less work than rebuilding AD and all its data.

Obviously, this solution isn't well-suited for a large multinational forest because it would create a tsunami of change verifications. It's also not well-suited for a call center Help desk that does password resets because the new passwords need to be immediately available to users.

However, this solution is well-suited for

- Organizational units (OUs) that contain highly visible accounts, such as the CIO's account.
- Small AD environments in which untrained staff work as AD administrators.
- Small AD environments in which an erroneous change can be catastrophic.
- Probationary administrators. (You can make sure that they know what they're doing before you let them loose.)
- Administrators of critical services, such as DNS.
- Configuration administrators of line of business (LOB) applications that store data in AD, where a mistake will make the application nonfunctional.

Using selective authentication in an external trust provides an effective solution for protecting AD objects from administrative errors. Although it requires some upfront work to set up, it can save you a lot of grief later on. As an advanced Microsoft feature, selective authentication is one more security tool that you can pull out of your bag of tricks.

—James R. Day, senior system engineer, NuAxis

InstantDoc ID 102765

## Dnscmd Versions Discrepancy

You can automate creating an Active Directory (AD)-integrated zone with forest-wide replication using the Dnscmd utility. However, you must use version 5.2.3790 or later of the Dnscmd utility, which you can find in the Windows Support Tools for Windows Server 2003 (32-bit).

If you're using the correct version of Dnscmd, the following command will create a new AD-integrated zone through a server named DNSSERVER:

```
dnscmd DNSSERVER
  /zoneadd 80.16.172.in-addr.arpa
  /dsprimary /dp /forest
```

Unfortunately, if you try to use this same command with version 5.1.2600 of Dnscmd, which is in the Windows Support Tools for Windows XP, Dnscmd will silently ignore the /dp switch. Furthermore, this version of Dnscmd will set the zone to replicate only to domain controllers (DCs). If you have any DNS servers that aren't DCs, they won't receive replication updates. (Although this sample command creates a reverse zone, the problem pertains to creating both reverse and forward AD-integrated zones.)

If you're trying to automate zone creation from the command line or a batch file, you can't use the command-line Help file to ensure you have the correct version of Dnscmd. Both versions claim to support the directory partition syntax and will show the Help information in Figure 1 for the /dp switch.

Despite what the command-line Help file states, version 5.1.2600 of Dnscmd will neither set up forest-wide replication nor replicate to non-DC DNS servers. So, if you're working from an XP system, check the version of Dnscmd you have before creating a DNS AD-integrated zone. As Figure 2 shows, you can find the version on Dnscmd's properties page. If you don't have version 5.1.2600 or later and you don't have the Windows Support Tools for Windows 2003 (32-bit), you can download Dnscmd from the "Windows Server 2003 Service Pack 1 32-bit Support Tools" web page (www.microsoft.com/downloads/details.aspx?familyid=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en).

—Rick Sheikh, IT consultant

InstantDoc ID 102795

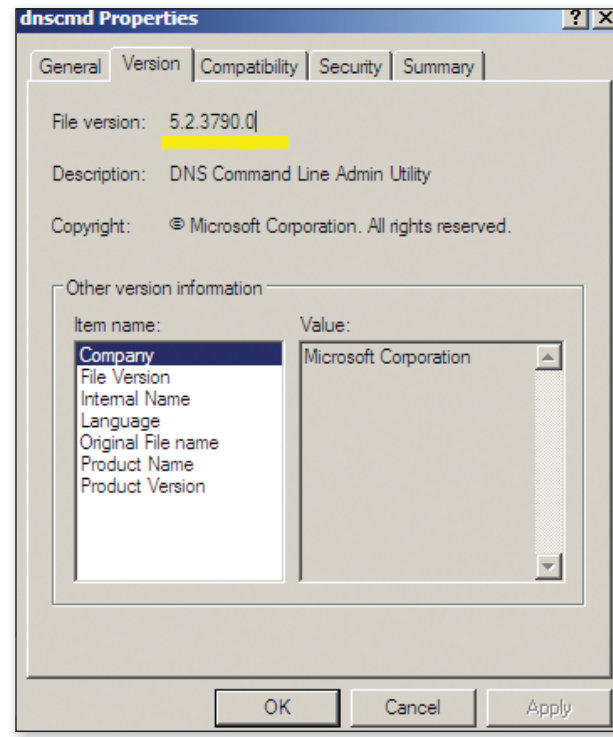



Figure 2: Finding the version of Dnscmd

- User Rights
- Outlook
- Hyper-V
- Windows 7

# ANSWERS TO YOUR QUESTIONS

## Q: How can I configure and manage Windows user rights from the command line?

**A:** You can use the ntrights utility to grant or revoke Windows user rights to users and groups on a local or remote computer. You can configure both logon rights and privileges with the ntrights utility, which is included in the Windows Server 2003 Resource Kit and the Windows 2000 Resource Kit. For example, to grant ServiceAccount1 on computer MyComputer the Logon as a service right, you must run the command

```
Ntrights +r SeServiceLogonRight -u
ServiceAccount1 -m \\MyComputer
```

To revoke the Everyone group's right to Access this computer from the network, run the command

```
Ntrights -r SeNetworkLogonRight -u
Everyone
```

To display the user rights that have been assigned to the account you used to log on to a Windows system, use the whoami command line tool with the /priv switch. Whoami is included in the Windows 2000 Resource Kit and undled with Server 2003, Windows Vista, and Windows Server 2008.

You can use the ShowPriv utility to display a list of which users and groups have been assigned a particular user right on your systems. ShowPriv is included in the Server 2003 Resource Kit and the Windows 2000 Resource Kit. Showpriv SeInteractiveLogonRight will, as an example, let you find users and groups that have been assigned the Log on locally logon on your system.

—Jan De Clercq

InstantDoc ID 102499

## Q: How can I send calendar information from Outlook to a mobile phone using SMS?

**A:** In another column, InstantDoc ID 102160, I looked at the Microsoft Outlook Mobile Service (OMS), which allows users to send SMS messages to mobile phones using an SMS Service. Within the OMS configuration settings, if added to an Outlook profile, is the option to send calendar data to an SMS-enabled mobile device. People in an organization who don't come to the office every morning, and who don't use an alternative synchronization application or protocol such as ActiveSync, should find this feature particularly useful.

When you install OMS, it adds commands to the standard Office Outlook 2007 menus. A section labeled Mobile is added to the Preference tab under Tools, Options. Click Notifications to open the Outlook Mobile Notification dialog box. At the bottom of this dialog box is a check box you can select to send a copy of the daily calendar to a wireless number using SMS. Note that this feature sends the next day's calendar. The drop-down box where you select the time isn't customizable—you must choose a time from a list that incorporates 30 minute increments on the hour and on the half-hour.

On the receiving end, the user will see by default a single SMS message for each calendar item sent. If there are six meetings, then the user should receive six SMS messages for the day. To send without this separation, uncheck the check box next to Send one single mobile message per appointment or meeting request.

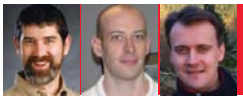
## Q: Does a pass-through disk for Hyper-V have to be direct attached storage on the Hyper-V host?

**A:** No. A pass-through disk is any storage that is accessible to the Hyper-V server, such as direct attached or a LUN on a Storage Area Network. Remember that regardless of where the storage is, it must be offline on the actual Hyper-V server before the guest can be configured to access it via pass-through. Also remember that the entire disk is mapped to a guest, not a volume on the disk. Finally, the disk must be initialized before it can be used for pass-through, so if the disk isn't initialized then initialize it on the Hyper-V host then place it in an offline status so it can be used for pass-through.

Normally you use Virtual Hard Disks for virtual machine storage. When configured as fixed size, VHDs perform almost identically to pass-through storage, and you lose features such as snap-shotting when using pass-through, so always try and use VHD above pass-through.

—John Savill

InstantDoc ID 102562



William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Jan De Clercq | jan.declercq@hp.com

This will use up all 160 characters of an SMS message before adding another. Either way, a full daily calendar may be spread over many SMS messages. This is important if your SMS service plan charges per message.

There's an option to exclude all-day events; these events often don't have a specific location or requirement for user response. By default, recurring events with instances on the weekend are omitted. Finally, the calendar items sent to the mobile device can be restricted by the time of the appointment. By default, this feature sends only calendar items falling between the common office hours of 9 A.M. through 5 P.M. If you schedule the calendar appointments to be sent at 5 A.M. it will send the next day's calendar, not the current day's appointments, to the user. This is the only mistake I've seen administrators make with this feature.

—William Lefkovics

InstantDoc ID 102337

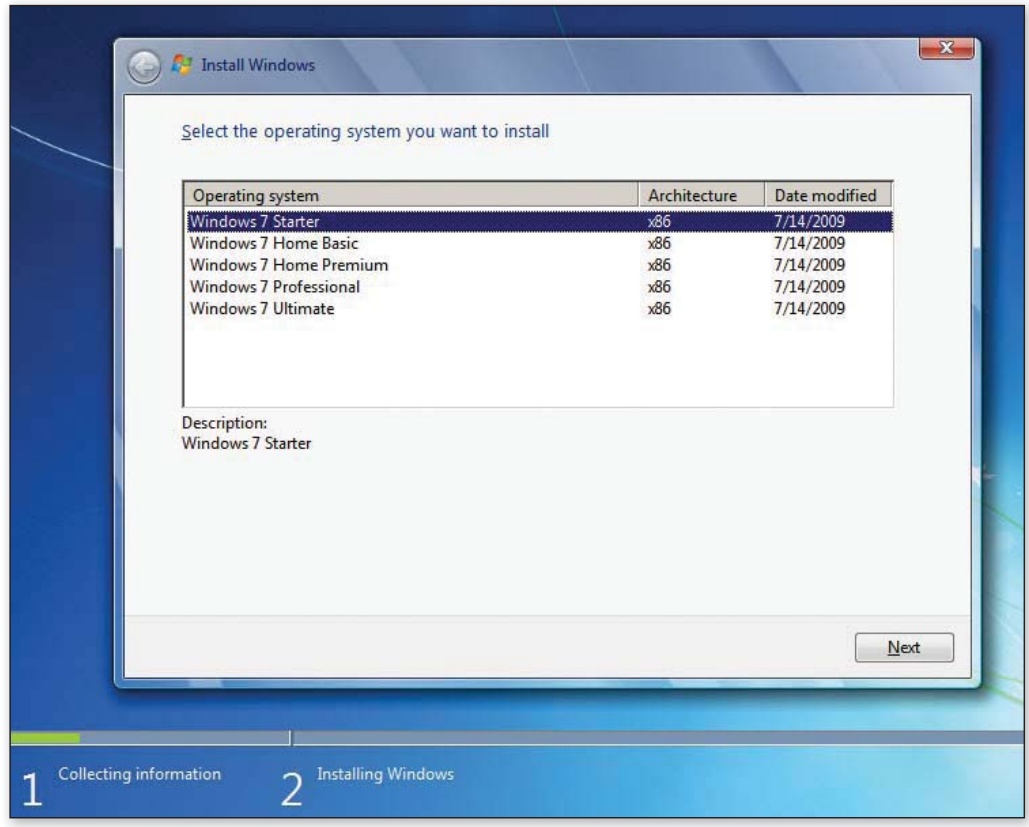



Figure 1: Windows 7's version select screen

## Q. Do I need to download all the different versions of Windows 7 from MSDN?

**A:** MSDN provides a different ISO for each version of Windows 7 (e.g. Ultimate, Professional, Starter) but they're all the same ISO. The only difference is that there's a file (ei.cfg) in the sources folder that tells the setup routine which image to select. You could, therefore, open the ISO, remove this file, and save the ISO. When you install from this ISO, you'd be prompted for which version of Windows 7 you want to install, as shown in Figure 1. You do, however, still need to download the x64 and x86 versions of Windows 7 if you want both the 32-bit and 64-bit versions.

You could also create multiple ISOs and modify the content of ei.cfg. The format is

```
[EditionID]
<version>
[Channel]
Retail
[VL]
0
```

So just change <version> to Ultimate, Professional, HomePremium, HomeBasic, or Starter. See Microsoft's site at tinyurl.com/lhhvgl for more information on ei.cfg

—John Savill

InstantDoc ID 102658

## Q: Does Microsoft provide a mechanism to restrict which administrators can manage a particular Hyper-V virtual machine (VM)? I want to make sure that VM administrators can only manage their VMs and can't touch the parent partition.

**A:** You can use the Authorization Manager (AzMan) to define specific roles for VM administrators on a Hyper-V server, and to ensure that they have permissions only for their respective VMs.

Microsoft first introduced AzMan in Windows Server 2003 so that developers and administrators would be able to add role-based access control (RBAC) rules to their applications more easily. Unfortunately, few Windows administrators have used AzMan and knowledge about how to configure it is fairly rare. For an excellent description of how to set up AzMan for delegating permissions on a Hyper-V server, see the blog at tinyurl.com/nsdksb.

In this context, it's worth mentioning System Center Virtual Machine Manager (VMM), Microsoft's enterprise management solution for virtualization servers and VMs. VMM reduces the complexity of configuring and managing AzMan authorization rules. More information about VMM is available on Microsoft's site at tinyurl.com/6reqdn.

—Jan De Clercq

InstantDoc ID 102497

Microsoft | Virtualization

SIMPLIFY AND ACCELERATE WITH MICROSOFT VIRTUALIZATION SOLUTIONS

HOW FAR WILL YOU TAKE VIRTUAL?

microsoft.com/virtualization/solutions

# TOP 8 REASONS

## for Implementing End-to-End Site Recovery Solutions Using Windows Server® 2008 with Hyper-V™

Virtualization has changed the way IT looks at cross-site disaster recovery. In the past, ensuring cross-site business continuity required a significant investment in hardware and software, including dedicated physical servers and storage infrastructure at multiple sites. With virtualization, you can reduce the amount of dedicated hardware required and the associated investment. Businesses that have committed to implementing Site Recovery (SR) solutions can gain greater value for their investment. And for companies previously unable to justify investment in SR, the return on investment can be significantly improved.

### 1. Integrated end-to-end solutions

Along with leading storage providers, Microsoft is delivering end-to-end site recovery solutions that leverage Windows Server® 2008 Failover Clustering, Hyper-V™, and integrated physical and virtual management through the System Center suite—including Microsoft System Center Virtual Machine Manager 2008 (VMM). By combining Hyper-V, Failover Clustering, and integrated management with storage partner data replication, Microsoft virtualization customers achieve robust, high-value, cost-effective site recovery solutions.

### 2. Connecting geographically dispersed sites

Clustering technology in Windows Server 2008 has been improved and redesigned; new features make it simpler to implement and use. By utilizing stretch clustering, IT Professionals ensure the availability of their host infrastructure between locations. Working with storage partner data replication, Microsoft delivers site recovery failover across geographic areas to protect against catastrophic failure at a primary location. With greatly expanded support for failover clusters, VMM 2008 improves its high availability capabilities for managing mission-critical virtual machines. VMM 2008 is now fully cluster-aware, meaning that it can detect and manage Hyper-V host clusters as a single unit. Managing VMs through VMM is completely seamless and managing highly available VMs is the same as managing VMs on a stand-alone system.

### 3. Build on existing skills and investment

Microsoft customers have been using Windows clustering technology for more than a decade. And with the release of Windows Server 2008 and Hyper-V, with failover clustering, Windows Server users have the tools in hand for implementing site recovery solutions that extend their existing investment in a Windows Server IT environment. Although users can choose manual-only failover, Windows Server clustering supports automatic failover and failback between primary and recovery sites, a solution that achieves a low Recovery Time Objective (RTO).

## 4. Integrated management for physical and virtual environments

The Microsoft System Center suite provides integrated management for physical and virtual environments—from core components such as Microsoft Systems Center Operations Manager, which you can use to provide overall operational information about your computing environment, to specific tools such as Microsoft System Center Virtual Machine Manager 2008, which simplifies migration to, and management of, virtualized environments. To ensure business continuity VMM also offers Performance and Resource Optimization (PRO), dynamically responding to failure scenarios and situations where performance is not optimized or to poorly configured components identified in hardware, operating systems, or applications. This is beyond simple alerting; PRO can perform a range of tasks including load balancing and automated migration of virtual machines to a different physical host.

## 5. Other features in Windows Server 2008 R2

With the high availability capabilities built into Windows Server, you can design an infrastructure that provides a robust, reliable shared-storage solution that offers built-in redundancy and tight integration with virtualization. For example, the Microsoft MPIO framework provides high availability and dynamic load balancing to SAN devices through redundant network or fabric connections. Microsoft MPIO dynamically routes IO to the best path and protects against failures at any connection point between a Hyper-V host and shared storage.

## 6. Ability to leverage Live Migration support

With the support for virtualization and stretch clustering in Windows Server Failover Clusters in Windows Server 2008 and the Live Migration support added by Microsoft System Center Virtual Machine Manager you already have the ability to do live migration not just between servers (physical or virtual) in the same datacenter, but between sites as well. This is a key component for a business continuity or disaster recovery solution. It's also a practical solution to the problem of migration to new or upgraded datacenters, or data center consolidation concerns.

## 7. Versatile partner ecosystem

A broad range of companies are partnering with Microsoft to offer solutions that build on and extend the capabilities of Windows Server 2008 to deliver end-to-end site recovery solutions. Solutions from Microsoft's extensive partner ecosystem leverage the capabilities of Windows Server 2008 R2 Hyper-V Failover Clustering and the System Center suite to provide integrated solutions for dispersed multi-site environments. Failover Clustering and Microsoft's partner ecosystem have been in place a long time and have proven to be a successful combination for many types of workloads.

## 8. Business benefits

Taking full advantage of Hyper-V along with failover clustering technologies already available in the Windows Server software means that you can deploy a much more flexible business server infrastructure, at little to no additional expense. Making use of Windows Server 2008 Failover Clustering and virtualization with Hyper-V gives Windows Server IT departments the ability to deploy, manage, and maintain highly available and cost-efficient server systems that are flexible and effective at addressing ongoing business needs.

.

# AD GOLD NUGGETS

## Dig out these little-known Active Directory Tools

by Sean Deuby

Like any complex system, Active Directory (AD) and its related support tools have numerous commands and techniques to make administration a bit easier and more efficient. As you acquire AD skills and knowledge, your toolkit will grow larger and you'll branch into using less-well-known tools and methods. In this article I present several AD nuggets you might not have discovered yet.

### Free GPO Disaster Recovery

Backup and recovery is a key area any AD administrator must pay attention to. But just instituting a domain controller (DC) backup and recovery plan isn't enough. You also need a separate backup and recovery plan for Group Policy. Unlike DCs, Group Policy Objects (GPOs) are typically delegated to a larger group of organizational unit (OU) administrators, rather than just the overall AD service administrators. The more people who work with GPOs—especially relatively inexperienced admins—the greater the chance that a GPO will be accidentally (or intentionally) altered or deleted. Because changes to a production GPO almost always affect multiple users, restoring the GPO quickly is a high priority. You can restore a GPO from DC backups, but the process can be slow and obtrusive.

Setting up basic GPO backup and recovery is easy. Group Policy Management Console (GPMC), which is included in Windows Server 2008 and Windows Server 2008 R2 and available as a download for Windows Server 2003 (at http://bit.ly/4DpDVp), has a great library of 32 sample scripts to perform Group Policy maintenance. After you install GPMC in Server 2003, these scripts are located in C:\Program Files\GPMC\Scripts. Although Server 2008 and R2 no longer include the scripts by default, they will work with these OS versions. You can download the scripts from Microsoft at http://bit.ly/1Jef98. In Server 2008 and R2, the scripts will install in C:\Program Files\Microsoft Group Policy\GPMC Sample Scripts. All the scripts let you perform various useful operations on GPOs; but the backup and recovery scripts we're interested in for the purpose of this discussion include BackupGPO.wsf, BackupAllGPOs.wsf, RestoreGPO.wsf, and RestoreALLGPOs.wsf. From an AD administrator's viewpoint, we're most interested in BackupAllGPOs to back up all the GPOs in a domain and RestoreGPO to restore a single GPO.

The scripts are written in either VBScript or JScript. If cscript.exe isn't your default scripting host, you'll need to explicitly specify cscript.exe on the command line. To back up all the GPOs in your domain, navigate to the script directory and run

```
Cscript backupallgpos.wsf <BackupLocation>
  [/Comment:<Comment>] [/Domain:<DNSDomain>]
```

The script will back up all the GPOs in your domain to the location you specify and create subfolders for each GPO, named by the 128-bit GUID that uniquely identifies the GPO. Once you've backed up all the GPOs, you can use RestoreGPO.wsf to restore them individually:

```
Cscript restoreGPO.wsf <backup location> <GPO name> /
  domain:<DNSDomain>
```

Although these scripts will back up and restore both the GPOs in AD and the Group Policy templates on SYSVOL, they don't back up or restore the links between the GPOs and the OUs they're applied to. You must track these links separately, or you can use the ListSOMPolicyTree.wsf script to list the relationships between the GPOs and the site, domains, and OUs they could be linked to.

### Monitoring FRS

An area related to Group Policy is SYSVOL, the folder structure on every DC that contains the domain's Group Policy templates and logon scripts. A replication mechanism—File Replication Service (FRS) in Server 2003, Distributed File System Replication (DFSR) in Server 2008 and R2—ensures that the SYSVOL structure stays synchronized between all the DCs in a domain. Using DFSR for SYSVOL replication is a huge improvement over the trouble-prone

FRS replication method. However, because DFSR requires both Server 2008 and a manual FRS-to-DFSR upgrade process, the majority of production domains still run FRS.

You should monitor FRS for two reasons. First, a properly functioning SYSVOL is critical to a healthy domain. However, most AD administrators don't proactively check or monitor FRS—partly because FRS Event Log messages are infrequent and not especially informative, and partly because FRS problems take a while to surface. Second, you need to ensure that FRS is functioning properly before you attempt an upgrade to DFSR replication, or you might corrupt your SYSVOL.

Microsoft has an FRS monitoring tool called Ultrasound, which you can download at http://bit.ly/gMy6S. An unusual name for a Microsoft utility, the tool was christened Ultrasound because it was the successor to a simpler tool named Sonar. (Don't ask me how Sonar got its name.) Ultrasound consists of three major components. One component is a small Windows Management Instrumentation (WMI) provider that's installed on every DC. It gathers FRS status information and sends it to the next component: the Ultrasound controller. This component consists of a service and a database that holds the FRS status data the controller pulls from the monitored servers. The database can be either Microsoft SQL Server Desktop Engine (MSDE—which you can download at http://bit.ly/20HiM) or SQL Server, and it doesn't have to be on the same system as the controller. The final component is the Ultrasound administrator's console, which must be installed on the same system as the controller component. This is where you can add and remove members (DCs) that are being monitored and view the general health of the monitored FRS set. You can also drill down into a great level of detail. Because the administrative console is limited in where it can run, keeping it constantly open for operators is inconvenient and probably unnecessary. I recommend that you install it, use it to clean up any existing SYSVOL replication problems, then revisit it once a week. Although Ultrasound has been around for a while, and it has the unique look and feel of a tool that grew out of Microsoft's Product Support Services (PSS) group, it gets the job done.

## NTDSUTIL Scripting

We all use NTDSUTIL for relatively common tasks, such as metadata cleanup from unplanned DC failures. But did you know that you can build simple scripts to run NTDSUTIL actions in the task scheduler or interactively? Simply list the NTDSUTIL commands one after another on a single line. If the command has multiple arguments, enclose them in quotes.

A good script example is the AD snapshot feature available in Server 2008. This feature lets you use the Volume Shadow Copy Service (VSS) to create a snapshot of a domain's data. You create the snapshot with the NTDSUTIL "snapshot" command. You can then use this information to quickly restore an object and all its attributes (including the hard-to-restore backlinks such as memberOf), through a combination of tombstone reanimation and PowerShell scripts.

For the snapshot feature to be useful, however, you must take snapshots on a regular basis. NTDSUTIL scripting lets you easily do so with the following one-line script:

```
Ntdsutil snapshot "activate instance
  ntds" create quit quit
```

Figure 1 shows the output from running this script. Add this script to Task Scheduler in a batch file. Similarly, you can create a script to view all the available snapshots, which is useful when you're in a hurry to restore an object:

```
Ntdsutil snapshot "act inst ntds
  "list all" quit quit
```

You can then quickly look through the listings to determine which snapshot you want to mount with the database mounting tool (dsamain.exe, available at http://bit.ly/X4prc).

## Preventing Accidental Deletion of OUs

Much of an AD administrator's job involves one simple task: preventing accidental deletion of AD objects. The difficulty of this task is directly related to the number of people who have rights in the domain. A good AD security model includes some speed bumps to minimize this risk. Although these practices don't constitute a complete solution by themselves, the "defense in-depth" principle ensures that their cumulative effect will make the domain a little safer.

One such speed bump is using AD's own access control to prevent accidental deletion of OUs. Although security principals (users, groups, and computers) in an OU come and go, OUs are part of an organization's structure and are rarely deleted. Starting with Server 2008, the Microsoft Directory Services Team made it easy to do what experienced AD admins had already been doing on their own: setting a Deny ACE (i.e., access control entry) on objects to prevent them from being inadvertently deleted.

In the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in, you can enable a setting to protect an object from accidental deletion, as Figure 2 shows. This check box, located

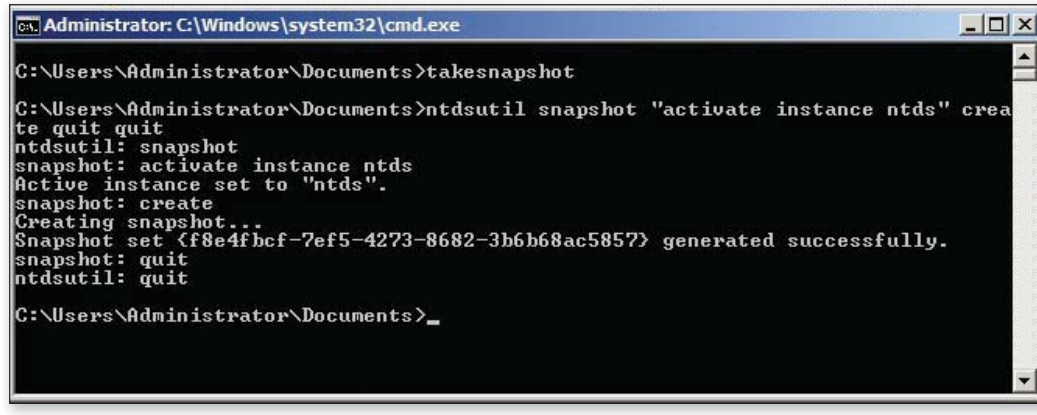



Figure 1: Running an NTDSUTIL script to take regular snapshots

in the OU Properties page's Object tab, sets Deny ACEs for the Delete and Delete Subtree permissions for the Everyone group. The check box must be clear for a deletion to take place.

You need to be aware of a few details when using this feature. First, this check box applies only to OUs. You can create, modify, and delete security principals in the OU with no problem. Second, the feature lacks inheritance—in other words, if you enable the feature for the top-level OU of an OU structure, it applies only to the OU for which you enabled it, not the OUs beneath that one. Although you can use .NET to write a script to apply the feature to other OUs, unless you have a particularly large OU structure, selecting the check box manually will probably take less time than writing (and exhaustively testing) a script. Because this feature sets a Deny ACE, you can apply this protection to any object in AD, but only the New OU wizard features an easy-to-use check box.

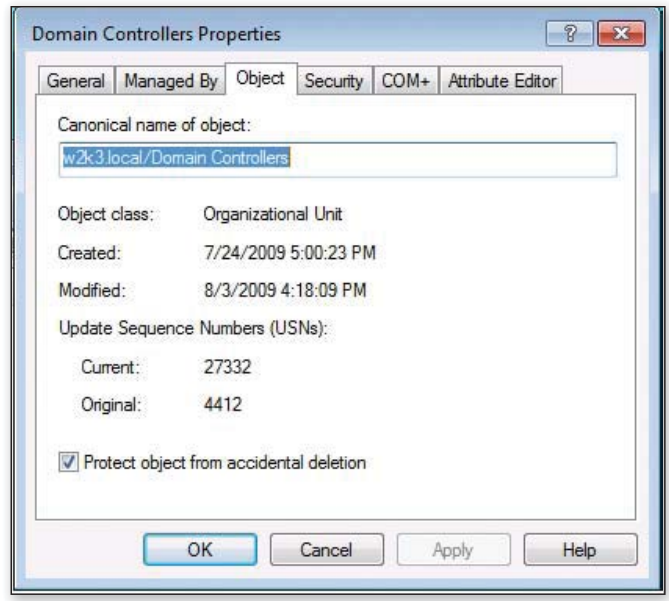



Figure 2: Preventing accidental deletion of an object

## Attribute Access for Everyone

One of the AD challenges that small and medium-sized companies face is correctly populating data without the use of expensive add-on tools. AD is pre-populated with an attribute for practically everything you can think of—and a few things you can't (e.g., Telex-Number). The employeeID attribute is intended to store an employee's unique ID number. However, there's no place in Active Directory Users and Computers where this attribute is exposed. An HR staff member or account administrator adding a new employee must use command-line tools such as dsmod or joeware's admod. Most account administrators aren't comfortable working with distinguished names (DNs), so a simple UI solution would be nice. Fortunately, an update to Active Directory Users and Computers for Windows 7 and Windows Vista provides an answer. The Remote Server Administration Tools (RSAT) for Vista (http://bit.ly/cnwzD) or Windows 7 (http://bit.ly/TYGxd) features an updated version of Active Directory Users and Computers (dsa.msc) with a welcome new feature: the Attribute Editor.

The Attribute Editor adds a key bit of functionality that's in ADSIEDIT or the LDP editor, but not in the familiar Active Directory Users and Computers interface: You can edit any AD object attribute, not just the ones the Active Directory Users and Computers interface traditionally exposed. Using our previous scenario, Figure 3 shows how to add an employee ID number to the new employee Sosumi Areti (the new staff Liability Director). By default, the Attribute Editor shows only a subset of all attributes for the object. You can filter the attribute list by whether they have values, are writeable, are mandatory or optional, are constructed, are backlinks, or are system-only. The ability to expose a constructed attribute can be very handy; if you're using fine-grained password policies in Server 2008, you can expose the effective password setting (effectivePso) for a user. Doing so is analogous to looking at the resultant set of policies for a user if you want to see what GPOs are affecting the user.

In addition to installing on Windows 7 or Vista, the Attribute Editor requires that you upgrade your Server 2003 forest schema to Server 2008 to update the forestwide display specifiers. An alternative manual

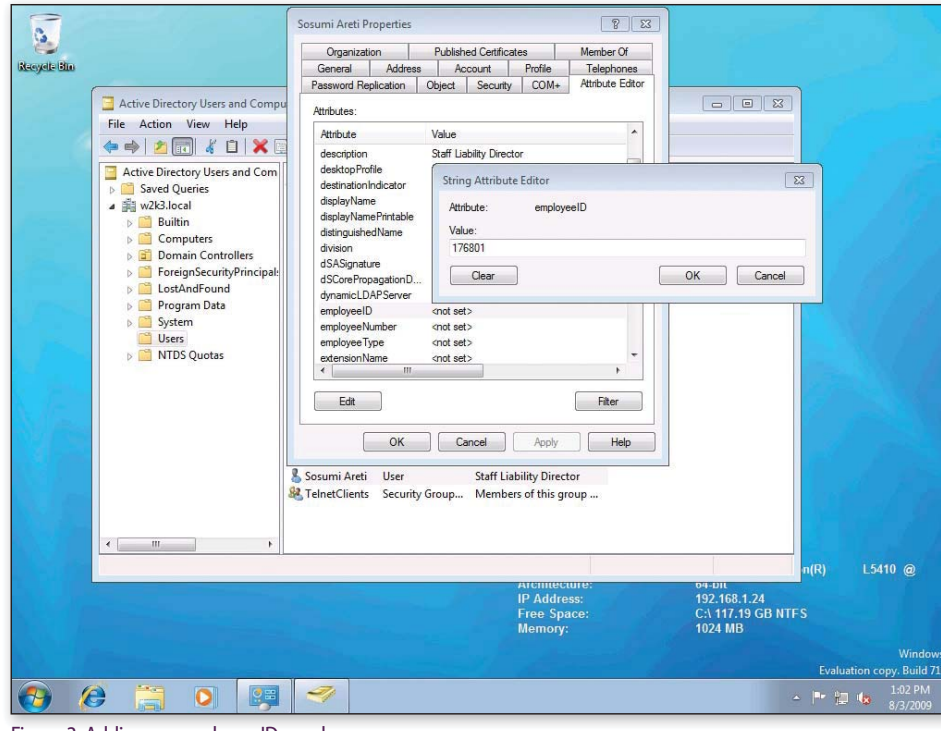



Figure 3: Adding an employee ID number

workaround is available at http://bit.ly/ysFP1.

Note that the RSAT installation works differently in Windows 7 and Vista than in Windows XP and Server 2003. When you install the toolset, the Start menu doesn't change—nothing appears to have installed. To make the tools appear, open the Control Panel Programs and Features applet, select *Turn Windows features on or off*, select Remote Server Administration Tools, Role Administration Tools, and drill down to the Active Directory Domain Services (AD DS) tools. (I encountered an R2 bug that requires you to check each tool individually, which I hope is fixed in RTM.) Finally, check the Advanced section of the View menu to see the Attribute Editor.

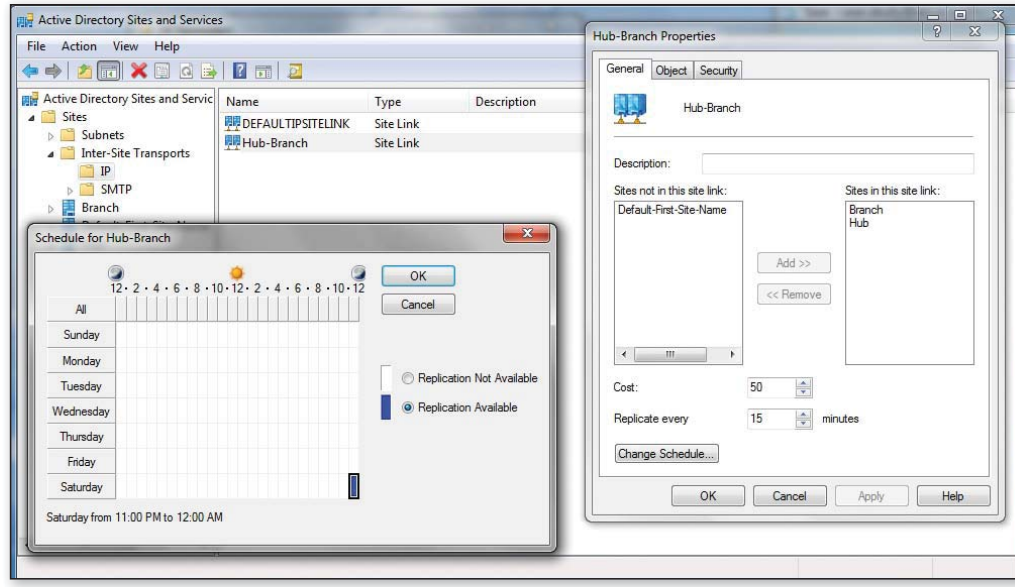



Figure 4: Using Active Directory Sites and Services to disable replication

## Controlling Replication

Although AD replication typically works well without administrator intervention, every AD administrator should know how to control it manually. Suppose that you accidentally delete an object and don't notice it right away. Being able to quickly stop replication outside your site will prevent the deletion from affecting outside users. Several replication control methods are available.

The best-known method is to use Active Directory Sites and Services (dssite.msc) to manage AD's sites and site links. Site links are the pathways upon which data is replicated. Start Active Directory Sites and Services and navigate to Sites, Inter-Site Transports, IP, then open the properties of the site link on which you want to disable replication, as Figure 4 shows. Click Change Schedule, select the entire range of days and hours in the schedule grid, and select Replication Not Available. This action disables replication between all sites that use the site link.

Using Active Directory Sites and Services disables replication only at the site level. You might need to disable replication at the DC level as well, perhaps to isolate schema changes or accidental deletions (if you're quick and have a script already set up). To disable replication at the DC level, you need to use the kitchen sink of replication tools—REPADMIN.

REPADMIN has so many command switches, sub-options, and complexities that someone could write an entire book about it. For this article, let's focus on the /options switch. If you use the standard /? switch to search REPADMIN's help files, you won't even see the /options switch. You must use /experthelp, which lists the more powerful switches that Microsoft clearly states "could break your Active Directory installation." And if you're running Server 2008, using /options is even more complicated; you must enter repadmin /?:options.

Once you figure out REPADMIN's syntax, it's the same for Server 2008 and Server 2003. Although replication is always a "pull" operation—meaning that a DC will always request replication to it, rather than push replication out from it—you'll typically want to disable outbound replication because it applies to our schema and object deletion scenarios. To disable outbound replication on a single DC, run

```
Repadmin /options <DC name>
  +disable_outbound_repl
```

If you want to disable outbound replication for multiple DCs, you'll have to write a simple script. To re-enable replication, change the "+" to a "-" and rerun the command.

The one exception to the REPADMIN /options command is that in Server 2008 you can disable outbound replication for an entire site—which is *very* handy in case of accidental deletion:

```
Repadmin /options site: <Site name>
  disable_outbound_repl
```

Several other advanced methods exist for controlling replication between individual DCs or groups of DCs, but they can be an administrative nightmare because the settings are so far outside where an AD administrator would typically look to resolve a replication problem. If you didn't clearly document the actions, your DCs might need to be entirely rebuilt. Even the /options method isn't easy for the casual troubleshooter to find. A solid production change-control process is extremely important.

## Obscurely Useful

AD is a complex structure with numerous tricks and tools to make administration easier. Some methods are more obvious and more widely used. The approaches I present in this article are less well known, but I hope they add to your arsenal of useful techniques for managing your AD environment.

InstantDoc ID 102733

**Sean Deuby**
(sdeuby@windowsitpro.com) is a contributing editor for *Windows IT Pro*, an enterprise solutions strategist with Advaiya, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.


# New Active Directory Features in Windows Server 2008 R2

## AD capabilities will turn any admin into "Super Admin"

by John Savill

Windows Server 2008 R2 is known for its new Hyper-V implementation with zero down-time migration capabilities. However, changes to Active Directory (AD) in Server 2008 R2 are almost as compelling and hint at this important infrastructure's future developments. The new AD features can be separated into two areas—manageability enhancements, and "everything else," which includes some very useful capabilities.

### Domain and Forest Functional Level Changes

Server 2008 R2 offers a new domain functional level, which you can enable after you have all Server 2008 R2 domain controllers (DCs) in the domain. It adds support for the new authentication mechanism assurance features we will discuss shortly.

Server 2008 R2 also offers a new forest functional level. It requires all DCs in the entire forest to be running Server 2008 R2 and adds support for the new Recycle Bin feature. Unlike previous Windows Server domain and forest functional level changes, moving here isn't one-way and can be reversed providing you haven't activated any feature that requires the domain or forest level. For example, if you've moved to the Server 2008 R2 forest functional level and haven't enabled the Recycle Bin, you could drop the forest functional level back down to the Server 2008 functional level. After you move to a Server 2008 R2 functional level, you aren't able to add Windows Server 2003 or Server 2008 DCs to the domain or forest.

Before you can introduce a Server 2008 R2 DC into a domain, you must perform a schema update as well as other tasks to be able to use certain new features in Server 2008 R2. If you're coming from a Windows 2003 domain as opposed to a domain already prepared for Server 2008, you'll also need to update Group Policy objects (GPOs).

In terms of co-existence, Windows 2000 SP4, Windows 2003, and Server 2008 DCs can exist in a domain with Server 2008 R2 DCs. Windows NT 4.0 BDCs aren't supported in a

domain with Server 2008 R2. Obviously as we start changing domain/forest functional modes we are restricted to the OS level of the DCs to match our domain/forest level.

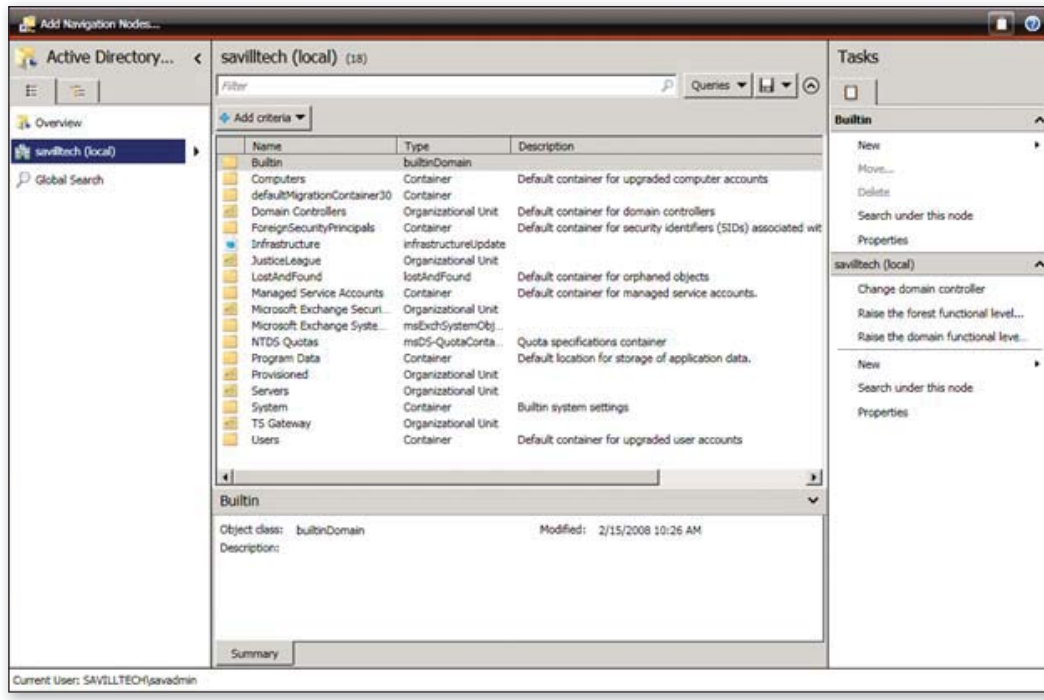


Figure 1: Active Directory Administrative Center home page

## Manageability Features

Server 2008 started the big push for Windows PowerShell-based management across the OS and services, but not all components had PowerShell support (many, in fact, did not). Server Core's new minimal installation mode with reduced footprint and attack surface didn't even support PowerShell because of the .NET dependency, which wasn't available on Server Core.

Server 2008 R2 remedies many of these PowerShell omissions. Server Core now supports many components of .NET, which means PowerShell is supported on Server 2008 R2 Server Core installations. Many roles and features that previously didn't support PowerShell now do, including AD.

The AD PowerShell implementation includes 75 PowerShell cmdlets and a PowerShell provider with an additional 14 cmdlets. Microsoft estimates that around 70 percent of AD functions can be performed with direct AD cmdlets written specifically to address the actions. The other 30 percent of these actions can be accomplished with PowerShell but not with dedicated cmdlets; instead, combinations of cmdlets are used.

## Active Directory Web Service

The new Active Directory Web Service (ADWS) is installed on Server 2008 R2 DCs; it operates over port 9389. The required firewall exception is enabled automatically as part of the role installation (including Server Core DCs); however, if you control firewall exceptions via Group Policy, you need to ensure you open this new port.

Currently most tools connect using LDAP and remote procedure calls (RPCs). However, offering a web service for AD access enables a superior developer experience and forms the first stage of a bigger objective, which is the enablement of AD for cloud and distributed service scenarios.

AD PowerShell cmdlets use the interface provided by ADWS. If a DC can't be found offering the ADWS, then the AD PowerShell cmdlets won't work. It's therefore very important that you have a sufficient number of R2 DCs running ADWS across all domains that a PowerShell cmdlet might query. Although you can disable ADWS, it's discouraged. Note that when Server 2008 R2 is released, an out-of-band update for Windows 2003 and Server 2008 will be released to add ADWS to these AD implementations.

## Active Directory Administrative Center

Active Directory Administrator Center (ADAC), which Figure 1 shows, is a new interface designed to replace Active Directory Users and Computers. In future server versions, ADAC will also replace AD Domains and Trusts and AD Sites and Services. It will offer a single administrative interface for all AD management along with support for features that currently don't have any graphical interface, such as Recycle Bin and fine-grained password policies (FGPPs).

ADAC lets you manage users, groups, computers, and organizational units (OUs) and offers powerful and intuitive search and filter options. Within a single instance, it lets you manage multiple domains and even connect to multiple DCs simultaneously.

ADAC is built on PowerShell but currently doesn't display the PowerShell commands that would be used to complete actions; this may be an option for a future version. ADAC consists of many layers; for example, it uses PowerShell, which, in turn, uses ADWS. ADAC's many new components and dependencies on the new 2008 R2 capabilities actually provide a very rich platform for AD management.

## Even More Great Management Features

In addition to the key features above, you'll also find more components related to management. Each is extremely useful in its own right.

***Active Directory Health Model.*** This is a single authoritative source for diagnostic information, which is used by the management packs and best practice analyzers. This health model can also be accessed by other third-party applications if necessary.

***Best Practices Analyzer (BPA) for Active Directory.*** This is available through

Microsoft



# More available, reliable, scalable. More able, period.

Upgrade now? Absolutely. Want built-in virtualization, significantly reduced power consumption and the ability to seamlessly move virtual machines without disruption of service or perceived downtime? Windows Server® 2008 R2 does that. Want simplified management through a single set of tools and enhanced protection for ubiquitous remote access? Who doesn't? Layer in the latest version of System Center and integrated Forefront™ security and you'll get all that too. Whew! That's a lot of added efficiency for one little ad.

To learn more about how server upgrades can create efficiencies, go to **itseverybodysbusiness.com/upgrade**

Snap this tag to get the latest news on server upgrades or text UPGRADE to 21710

Get the free app for your phone at **http://gettag.mobi**

**Because it's everybody's business**

Server Manager and allows the installation of the selected DC to be validated against all the AD best practices. It's a useful "quick access" check point to confirm configuration.

***Management Pack for Server 2008 and Server 2008 R2.*** Although not an AD feature, a new System Center Operations Manager 2007 management pack monitors all features related to Server 2008 and Server 2008 R2 AD implementations. See the Microsoft download page: www.microsoft.com/downloads/details.aspx?FamilyId=008F58A6-DC67-4E59-95C6-D7C7C34A1447&displaylang=en&displaylang=en.

## The Really Good Stuff

Server 2008 R2's new management features are nearly overshadowed by two new nonmanagerial functions of Server 2008 R2: Managed Service Accounts (MSAs) and the AD Recycle Bin.

***Managed Service Accounts.*** Service accounts—dedicated AD accounts that run a server service—are the longest-standing security vulnerability in AD. Because services such as SQL Server and Exchange depend on these accounts, changing their passwords will interrupt the service. To combat this problem, many installations opt to use built-in accounts such as the local system and network service accounts, which are then shared by many services. However, if one service is compromised, all the services using the same built-in account could be compromised. This has finally been fixed in R2 with MSAs.

MSAs in Server 2008 R2 are AD accounts that are designed to simplify password and Service Principal Name (SPN) management by automatically changing the account's password on the server when it's changed in AD. The SPN configuration is required for Kerberos to correctly function and currently must be done by a domain admin; with the MSA, you can delegate the SPN update to any user, along with the ability for the service to automatically update the SPN for its MSA. It should be noted that an MSA can be used on only one computer; there's no sharing between computers.

To take advantage of the password management capabilities of MSAs, you can have domains running in Windows 2003 or later, but they must have run the Server 2008 R2 forest and domain preparations. To access the SPN management capabilities, you must be running in Server 2008 R2 domain mode, which means using only Server 2008 R2 DCs. To use an MSA, machines must be running Server 2008 R2 or Windows 7.

When the Server 2008 R2 domain preparation is run, a new container is created called Managed Service Accounts. This is the default location for MSAs; however, you can change the location if needed. All management of MSAs is performed via PowerShell cmdlets both within AD and on the server side. After you add an MSA in AD, give it any required rights, and install it to a service, you configure the service on the host to use the MSA, and you're done.

A virtual account works in a similar fashion to an MSA but is a local machine account. It doesn't have any password management capabilities and doesn't use AD. You can think of a virtual account as just additional network service accounts that have their own profiles. You don't add or remove virtual accounts; you just tell a service to use a virtual account.

***AD Recycle Bin.*** Deletions happen within AD, sometimes caused by admin error. When this happens, you can boot into directory services restore mode and perform authoritative restores of certain objects, or you can try to reanimate the tombstoned object directly through utilities such as ADRestore from technet.microsoft.com/sysinternals.

Both approaches have their problems. An authoritative restore is a pain and requires taking a DC offline during the restore process (and you need a good backup). Reanimating a tombstoned object takes away most of the attributes of the object, and all linked value attributes are removed (such as group memberships).

With Server 2008 R2 AD, we can enable the Recycle Bin, which allows the restoration of any deleted object through a simple PowerShell cmdlet, Restore-ADObject. Currently it doesn't have a graphical interface; however, the PowerShell cmdlet still offers a lot of flexibility in restorations. When you restore an object from the Recycle Bin, all of the object's attributes, both linked and non-linked, are completely restored, which means group memberships are also restored.

To enable the Recycle Bin, you must be at the Server 2008 R2 forest and domain functional level. After you enable it, the feature can never be disabled.

A deleted object can exist in one of two states after you enable the Recycle Bin: deleted or recycled. When an object is first deleted, it goes into a deleted state and is stored in the Deleted Objects container with its distinguished name mangled. An object stays in the deleted state for the msDS-deletedObjectLifetime duration, which by default is the same as the tombstoneLifetime duration—180 days. Both of these default times can be changed.

After the msDS-deletedObjectLifetime has passed, the object becomes a recycled object, and most of its attributes are stripped away (including linked attributes). After an object is in a recycled state, it can't be restored—not via the Recycle Bin capabilities nor from an authoritative restore. The recycled state always wins: If you perform an authoritative restore of an object in a recycled state, it is placed back into that recycled state again. Once the tombstoneLifetime has passed, the object will be physically deleted via the garbage collection process.

Any objects that were in tombstone state at the time the Recycle Bin is enabled are automatically set into recycled state, which means you can't undelete them via the Recycle Bin or an authoritative restore (because their attributes were already mangled per normal pre-Recycle Bin functionality).

It should be noted that the Recycle bin is available for Active Directory Lightweight Directory Services (ADLDS) in addition to Active Directory Domain Services (AD DS).

## Provisioning, Security, and Migration

Sometimes you need to complete a computer provisioning including joining a domain in environments where a DC might not be available. A new feature called offline domain join lets machines join a domain without having to contact a DC over the network. The process uses a new command-line tool, Djoin.exe, which initially provisions the new machine with an account in AD and saves required information to a text file. The machine then uses the text file to be joined offline to the domain, and after a reboot, the computer becomes part of the domain. This is available only on Server 2008 R2 and Windows 7 computers.

A new feature called authentication mechanism assurance lets administrators add additional universal group memberships to a user's Kerberos token when a certificate-based logon method is used. Services can then check for this universal group membership in the user's token, which identifies details about the certificate-logon performed. Different universal group memberships can be set in the token based on the certificate issuance policy object identifier (OID). This is very useful in federated identity management situations (such as ADFS) and claims-consuming applications in general. The information in the token can be extracted to check the authorization level and to grant authorization appropriately, depending on whether a certificate-based logon method was used and the OID of the certificate. Authentication mechanism assurance requires Server 2008 R2 domain mode.

Lastly, Server 2008 R2 offers migration wizards and documentation to help migrate AD and DNS services to new servers. Since Server 2008 R2 is 64-bit, some companies will need to combine adopting Server 2008 R2 with a hardware refresh and possibly a virtualization platform.

The new migration wizards and documentation offer detailed guidance for the entire process. The migration portal can be found at technet.microsoft.com/en-us/library/dd365353.aspx.

## Deciding What To Do Next

Many organizations running Windows 2003 question whether they should adopt Server 2008 today or skip it and go straight to Server 2008 R2. Several different considerations can drive a decision to adopt Server 2008 R2.

You need to look at the feature sets available in the releases. Decide if the benefit of the feature warrants adopting Server 2008 today—for example, to take advantage of Read-Only DCs, Server Core, DFS Replication of SYSVOL, and FGPPs—or whether you can wait and jump straight to Server 2008 R2.

However, it's important to realize that the decision whether to migrate to Server 2008 or to Server 2008 R2 doesn't have to be "all or nothing." Many of the new Server 2008 R2 features can be obtained by implementing only a few Server 2008 R2 DCs while leaving the majority of DCs on Server 2008.

Obviously one of the most sought-after features, the AD Recycle Bin, is also the most complex and most expensive, requiring every DC in the entire forest to be running Server 2008 R2. The fact that Server 2008 R2 must run on 64-bit hardware might also be a deciding factor in your adoption decision.

InstantDoc ID 102483

**John Savill**
(john@savilltech.com) is an advisory architect for EMC's Microsoft consulting practice. He's an MCITP: Enterprise Administrator for Windows Server 2008 and a nine-time MVP. His latest book is *The Complete Guide to Windows Server 2008* (Addison-Wesley).

# Transport Rules and Message Classifications in EXCHANGE 2007

## Use these 2 features for greater administrative control over message flow

by William Lefkovics

Microsoft Exchange Server 2007 transport rules provide a rich interface to control messages based on certain messages properties. Microsoft made changes to Exchange architecture that have helped expose this functionality for easier administration and to provide better compliance and content control. Message classification complements transport rules as a means of tagging messages, either manually or automatically, for specific treatment. Outlook 2007 and Outlook Web Access (OWA) 2007 with Exchange 2007 bring this control to life.

### Exchange 2007 Changes Transport Architecture

With Exchange 2003 and Exchange 2000, Microsoft used the extensible SMTP engine of Microsoft Internet Information Services (IIS), running within the inetinfo.exe process, to provide Internet messaging services. Exchange used Component Object Model (COM)–based engines to integrate with IIS SMTP and provide programmatic access to the SMTP transport subsystem. SMTP event sinks provided the conduit between Exchange extensions of IIS SMTP and message transport. The coding required to implement a comprehensive event sink was beyond the scope of many Exchange administrators.

When Microsoft developed Exchange 2007, they rewrote the transport system from scratch in managed code. SMTP and message processing are now handled within Exchange by the Microsoft Exchange Transport Service (MSExchangeTransport.exe). The new architecture lets sequential agents access the SMTP stream at specific events. These SMTP Receive Agent events represent different commands and processes in an SMTP conversation. Table 1 outlines the different events exposed in the order they're met through an SMTP transaction.

### Transport Agents and Rules

Transport agents represent code that interacts with SMTP messages through class libraries provided by Exchange 2007. Agents can read and change message properties and content during SMTP Receive Agent events. Transport rules depend on specific transport agents: the Edge Rules agent on Exchange 2007 servers running the Edge Transport role and the Transport Rule agent on servers with the Hub Transport role installed. These rules agents act at the OnEndOfData event in the SMTP stream. Administrators assign direction to the rules agents through the use of transport rules.

An example of transport agents at work is exhibited by the set of antispam agents employed by an Edge Transport server as well as Exchange servers running the Hub Transport role with the optional antispam agents installed. The antispam agents act on message properties exposed through SMTP events and can amend an email

Table 1: SMTP Receive Agent Events

| Receive Agent Event | Description |
|---|---|
| OnConnect | Exchange receives an SMTP connection |
| OnEhloCommand | Exchange receives an SMTP EHLO command |
| OnHeloCommand | Exchange receives an SMTP HELO command |
| OnAuthCommand | Exchange receives an SMTP AUTH command, but before it responds |
| OnEndOfAuthentication | Exchange responds to an SMTP AUTH command |
| OnMailCommand | Exchange receives an SMTP MAIL command |
| OnRcptCommand | Exchange receives an SMTP RCPT command |
| OnDataCommand | Exchange receives the SMTP DATA command |
| OnEndOfHeaders | Exchange reaches the end of the headers for an SMTP message |
| OnEndOfData | Exchange reaches the end of data for an SMTP message |
| OnRsetCommand | Exchange receives an SMTP RSET command |
| OnReject | When any other event rejects a command or message |
| OnDisconnect | When an SMTP connection to Exchange is closed |
| OnNoopCommand | Exchange receives an SMTP NOOP command |
| OnHelpCommand | Exchange receives an SMTP HELP command |

message, reject a message, and even readdress a message. To view the transport agents installed on a server, you can run the Exchange Management Shell (EMS) command

```
Get-TransportPipeline
```

Figure 1 shows the output from running this command on an Edge Transport server. You can see where the antispam agents reside in the transport process as well as the Edge Rules agent at the OnEndOfData event.

Microsoft doesn't apply restrictions to transport agent behavior: They have significant access to message content and header information and therefore only trusted and tested transport agents should be deployed in production. For more information on transport agents, refer to the Microsoft article "Transport Agents" (msdn.microsoft.com/en-us/library/aa579185.aspx).

## Edge vs. Hub: A Tale of Two Roles

Transport rules can be managed through Exchange Management Console (EMC) as well as EMS. They can be implemented on Exchange 2007 servers hosting the Edge Transport role or the Hub Transport role. The method for administering transport rules on these separate roles is the same; however, the focus of the set of rules is different.

Transport rules on the Edge Transport role primarily contribute to message hygiene. The Edge Rules agent can protect your internal network from email-borne attacks, such as virus outbreaks or denial of service attacks. It can also prevent internal compromises from being escalated to your clients and other external contacts by identifying and blocking unwanted outbound messages. The Edge Transport server is an email gateway, so you can use transport rules here to help ensure content reaching users' Inboxes is relevant.

Edge Transport server rules are stored within the local implementation of Active Directory Application Mode (ADAM); therefore, where multiple Edge Transport servers are used, each one has an independent set of transport rules. ADAM is a somewhat portable subset of Active Directory (AD) and isn't replicated between servers. You can maintain identical, redundant Edge Transport servers hosting the same set of transport rules, or unique Edge Transport servers for managing specific traffic, such as separating inbound and outbound messaging gateways.

Transport rules on Hub Transport servers focus more on message compliance and policy enforcement. You can restrict or prevent email delivery between groups of users within the organization and ensure certain information doesn't get delivered to unintended recipients. Hub Transport rules can also be used to append content, such as disclaimers, to message bodies prior to submission to an outbound gateway server. These rules are stored in the Exchange Configuration container in AD. Because these transport rules are stored in AD and replicated to all domain controllers, all Hub Transport servers access the same set of transport rules. And because every message sent through an Exchange 2007 organization must pass through at least one Hub Transport server, every message has the Hub Transport rules applied to it. This situation provides a solid platform for meeting messaging compliance requirements.

There are three components to transport rules: conditions, exceptions, and actions. Conditions and exceptions are sometimes called predicates. Web Table 1 (www.windowsitpro.com, InstantDoc ID 102846) lists the predicates and actions available for Edge Transport and Hub Transport rules. Hub Transport rules have more options that give you greater control over message flow. Edge Transport rules identify message properties to help discern whether the message should pass freely, be amended, or even rejected.

The available options for transport rules might not meet the requirements of every organization, and they can't be edited. However, developers can make their own transport agents to meet requirements not met by the basic transport rule set.

Within transport rules, there are predicates that are dependent on a value called classification and an action that can assign a message classification to an email message based on properties of the message—so now we see how message classifications can be added to the mix to provide more granular control over your environment.

Tony Redmond covers transport rules in more detail in "Exchange 2007 Transport Rules" (windowsitpro.com/article/articleid/95996).

## What Are Message Classifications?

Message classification, similar to message categories in the Outlook client, is a means of labeling and differentiating messages. These classification tags can then be used within a transport rule so that specific actions can be invoked. Message classifications can be assigned by a Hub Transport rule or by user action before sending a new message. This feature is new to Exchange 2007 and available only with Outlook 2007 and OWA 2007. Previous versions won't recognize message classifications.

Exchange includes several preconfigured classifications. These samples can be changed or deleted, but they might fit your

Figure 1: Output from the Get-TransportPipeline command on an Edge Transport server

```
Event                                 TransportAgents
-----                                 ---------------
OnConnectEvent                        {Connection Filtering Agent}
OnHeloCommand                         {}
OnEhloCommand                         {}
OnAuthCommand                         {}
OnEndOfAuthentication                 {}
OnMailCommand                         {Connection Filtering Agent, Sender Filter Agent}
OnRcptCommand                         {Connection Filtering Agent, Address Rewriting Inbound
                                          Agent, Recipient Filter Agent}
OnDataCommand                         {}
OnEndOfHeaders                        {Connection Filtering Agent, Address Rewriting Inbound
                                          Agent, Sender Id Agent, Sender Filter Agent,
                                          Protocol Analysis Agent}
OnEndOfData                           {Edge Rule Agent, Content Filter Agent, Protocol
                                          Analysis Agent, Attachment Filtering Agent}
OnHelpCommand                         {}
OnNoopCommand                         {}
OnReject                              {Protocol Analysis Agent}
OnRsetCommand                         {Protocol Analysis Agent}
OnDisconnectEvent                     {Protocol Analysis Agent}
```

Figure 2: Output from the Get-MessageClassification command

```
ClassificationID              : d74dbde8-4cb0-4043-ae4b-2a1b5686c9dc
DisplayName                   : A/C Privileged
DisplayPrecedence             : Medium
Identity                      : Default\ExACPrivileged
IsDefault                     : True
Locale                        :
RecipientDescription          : This message is either a request for legal advice
                                from an attorney or a response by an attorney to
                                a request for legal advice. It should be treated
                                confidentially, should only be sent to people with
                                a need to know, and should only be forwarded by
                                an attorney.
RetainClassificationEnabled   : True
SenderDescription             : This message is either a request for legal advice
                                from an attorney or a response by an attorney to
                                a request for legal advice. It should be treated
                                confidentially, should only be sent to people with
                                a need to know, and should only be forwarded by
                                an attorney.
UserDisplayEnabled            : True
Version                               : 0
```

company's needs. They are as follows:

- A/C Privileged
- Attachment Removed
- Company Confidential
- Company Internal
- Originator Requested Alternate Recipient Mail
- Partner

The EMS cmdlet Get-MessageClassification with the format list output option can list the details of message classifications. Here's an example using the A/C Privileged classification (that's Attorney/Client, not Air Conditioning as it's apt to mean here in the Mojave Desert):

```
Get-MessageClassification
  "A/C Privileged" | fl
```

Figure 2 shows output from this command.

## Adding New Message Classifications

You create new message classifications on the server side for use by transport rules or by Outlook 2007 and OWA 2007 clients. You use the aptly named New-MessageClassification cmdlet through EMS to create message classifications. A few parameters are required as well. The message classification DisplayName parameter represents what users see in Outlook 2007 or OWA 2007 when selecting from the message classification list, as we'll see shortly. The SenderDescription and RecipientDescription fields are shown on messages that have been classified. You can see a complete list of parameters for the cmdlet in the Microsoft TechNet article "New-MessageClassification" (technet.microsoft.com/en-us/library/bb124400.aspx).

As an example, the command

```
New-MessageClassification -Name Articles
  -DisplayName Windows IT Pro
  -SenderDescription "This message
  contains information and content
  supporting Windows IT Pro magazine
  articles."
```

creates a message classification with the minimum required parameters; it has an identity of Articles and a display name of Windows IT Pro. The new classification is added to the Exchange Configuration container in AD. Of course, Message Classifications can be deleted in a similar manner with the Remove-MessageClassification cmdlet.

## Setting Up Outlook for Classifications

Outlook isn't automatically aware of message classifications. Classifications are stored in AD and need to be exported to an XML file for Outlook, which you can do with a PowerShell script found in the scripts folder in the Exchange 2007 installation path (\program files\microsoft\exchange server\scripts\export-messageclassification.ps1). When you execute the script, pipe the output to an XML file:

```
c:\program files\microsoft\
  exchange server\scripts\export-
  messageclassification.ps1 >>mclass.xml
```

Exporting multiple times to the same XML file appends the content instead of replacing it, which makes the file unusable by Outlook. You must use a unique name or remove any existing XML file by the same name before exporting.

Message classifications are available only with Outlook 2007 using MAPI or with OWA on an Exchange 2007 server running the Client Access role and accessing an Exchange 2007 mailbox. They aren't visible to Windows Mobile clients, other ActiveSync clients, or clients accessing Exchange with other Internet protocols, including POP3 and IMAP4. Classifications are defined in the exported XML file, but that file needs to be pushed out to clients. You could use a network share, but pushing the XML file to the actual workstation is recommended, especially if users work offline with Cached Exchange Mode.

You have to enable message classifications in Outlook 2007 on an individual client basis through the creation and configuration of a registry subkey, HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Policy. The subkey Policy doesn't exist by default and should only be created if the user's mailbox resides on an Exchange 2007 Mailbox server. You also don't need to enable clients that won't access the message classification system. In the Policy subkey, set the following values:

- "AdminClassificationPath"="c:\\Email\mclass.xml"
- "EnableClassifications"=dword:00000001
- "TrustClassifications"=dword:00000001

The full path and file name for the XML file must match what you assign using the AdminClassificationPath value in the registry.

## Step-by-Step Message Classification Distribution

Message classification in Exchange 2007 isn't a set-and-forget configuration for Outlook and OWA. Any changes or additions made to the classifications on the Exchange server require another XML export and redistribution to Outlook clients. As a mini-review, the steps to distributing or updating message classifications for use at the client are:

1. Add or change message classification through EMS

2. Run the export shell script to create the XML file for clients
3. Add registry subkey on clients that don't have it yet
4. Distribute the XML file to clients to the location defined in the local client registry
5. Restart Outlook if necessary

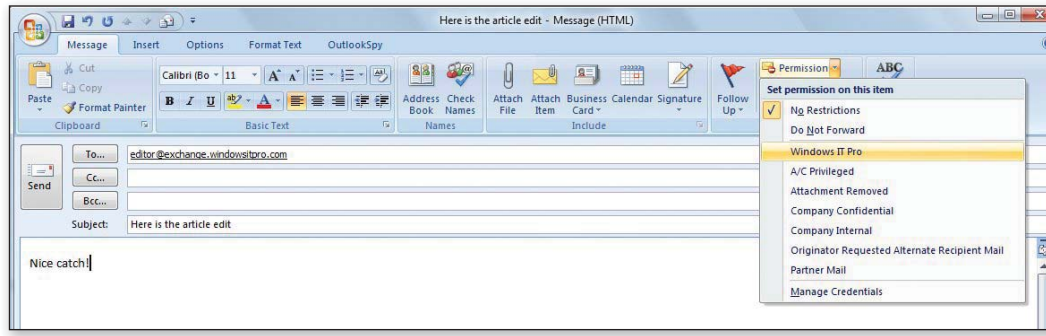



Figure 3: Selecting a message classification in a new email message

After these steps are completed, any changes or additions to message classifications can be used in transport rules to control message flow, maintain compliance, and enforce policy.

The requirement to manually create and distribute the XML file for message classification has been its Achilles' heel, limiting its adoption, especially for larger organizations. However, when a company establishes a solid set of message classifications and has them in place on Outlook 2007 clients, no further maintenance is required. It's only when changes need to be applied, whether adding a new classification or reinstalling a client workstation, that the tedious nature of message classification deployment arises.

There are tools within typical Windows networks that can assist in the distribution of updates to clients, including Group Policy and the Office Customization Tool for Office 2007. Some third-party application management products can apply registry changes and distribute files to workstations as well. Even with these tools, message classification adds administrative complexity that might not be worth the value of the deployed feature.

## Using Transport Rules with Classifications

Message classifications are a way for users and organizations to better describe messages. They aren't associated with any transport rule by default. With Hub Transport rules, you can control how messages move within your organization. These rules evaluate whether messages meet one or more conditions, then check whether they meet any exceptions. If a message passes through these predicates, then the configured action is taken. In each step—conditions, exceptions, and actions—there's an option for consideration of message classifications.

Let's put the sample message classification we created earlier, named Articles, to work. First, follow the steps outlined in the previous section. Add a recipient description using EMS as follows:

```
Set-MessageClassification
   -Identity Articles
   -RecipientDescription
      "Alert! Windows IT Pro Article
      Content!"
```

RecipientDescription is an optional parameter in message classification creation. Next, run the export script to create a new XML file with this change; if you have more than one change to make, it's more efficient to do them all before creating the XML file.

You should verify the changes by sending a test message and confirming the message classification works as expected. Create a new email message and select the new classification from the drop-down menu under the Permissions button, as Figure 3 shows. When this message classification is selected in Outlook 2007, the sender description text appears at the top of the message.

With this message classification in place, let's create a transport rule for illustration purposes. The goal of this rule will be to assign the classification Articles to messages sent to our internal editor address unless they're sent with low importance. In EMC, navigate to the Organization Configuration container and select Hub Transport. Recall that transport rules are stored in AD and apply to all Hub Transport servers in the organization. Select the Transport Rules tab, then click New Transport Rule in the Action pane to open the New Transport Rule wizard.

Transport rules must be assigned a name, but the description is optional. Click Next to go to the Conditions screen, select the check box for *sent to people*, and edit

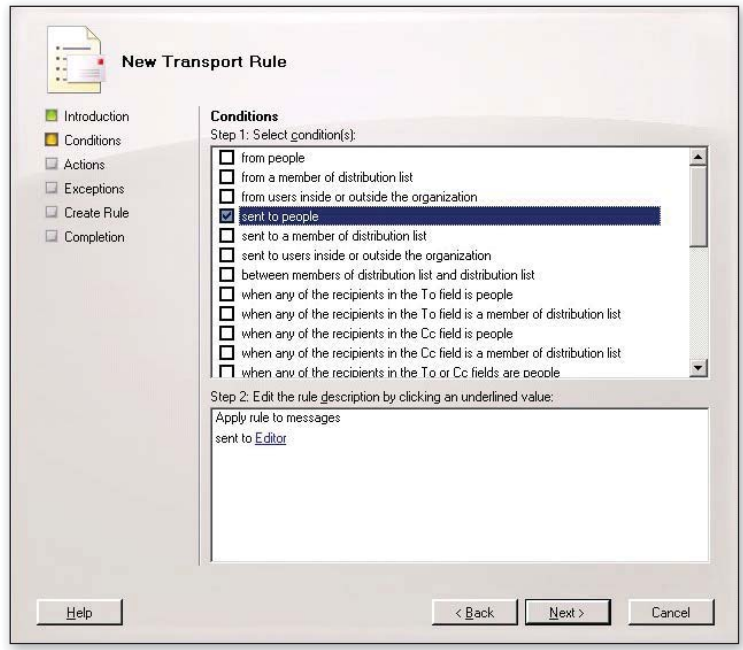



Figure 4: Setting a transport rule condition in the New Transport Rule wizard

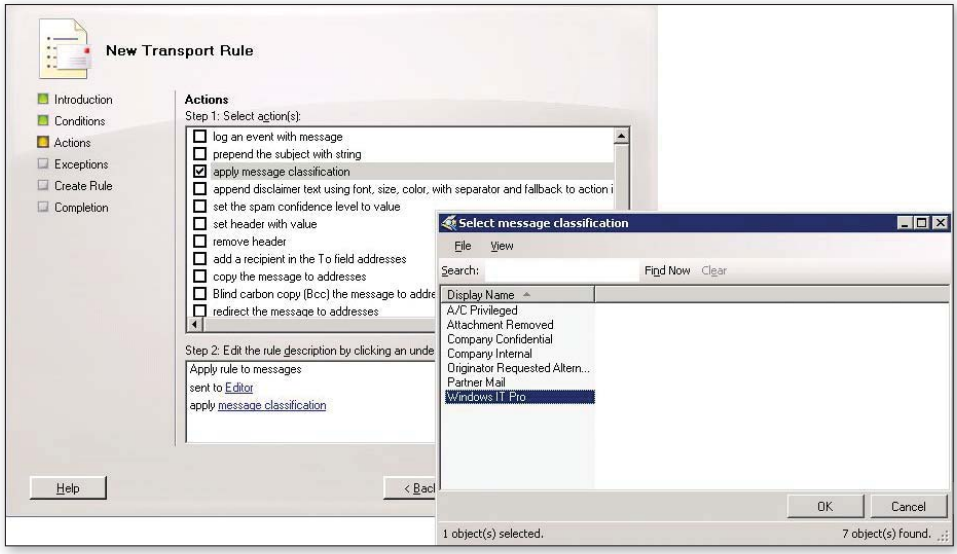



Figure 5: Selecting a transport rule action in the New Transport Rule wizard

the description so the rule is applied to messages sent to Editor, as Figure 4, page 37, shows. Next, the wizard displays the Action screen where you can assign the message classification Articles, selected by its display name of Windows IT Pro, to messages meeting the conditions of the rule, as Figure 5 shows. Now, this rule needs an exception for messages sent with Low Importance, which you can set on the Exceptions screen. Click Next to complete the new transport rule, and the final window shows the PowerShell command you could use to create this same rule through EMS.

To test this transport rule, you can send an email message without any message classifications assigned to it to the Editor mailbox and verify that the message is assigned the message classification when it arrives. Figure 6 shows the Recipient Description text applied by the message classification Articles, which was assigned to the test email by the transport rule.

The full set of Hub Transport rule conditions and exceptions shown in Web Table 1 is available for transport rules based on message classification. Transport rule actions can be applied based on the presence of a specific message classification, and a message classification can be applied to a message based on certain transport rule conditions. Messages to or from specific people or groups, messages with specific words or text patterns in addresses, message bodies, or header content, and even attachment name or size can all be used by companies to regulate message flow.

As an example, a small law firm in Vancouver uses message classifications and transport rules to separate important client communication into a resource mailbox, regardless of sender. Users assign message classifications before sending critical email messages to clients, and a transport rule copies the message to the resource mailbox based on the presence of the message classification and the recipient address.

Some companies might use message classification to emphasize the importance or confidentiality of an email message. The HR department could send out a message advising staff about changes in the health plan and select a message classification designed to display specific recipient text at the top of messages read in Outlook 2007 and OWA 2007.

## Rules and Classifications: Better Together

When you use message classification in the formation of Hub Transport rules, either as a condition, an exception, or an action, you get greater administrative control over message flow. Classifications can help you use transport rules to enforce corporate policy, adhere to compliance initiatives, and generally prevent email content from being distributed to recipients that shouldn't have access to it.

The system of transport rules isn't perfect, and the challenges of message classification distribution might prevent some companies from deploying the feature. Still, the full versatility of transport rules from enforcing ethical walls to appending disclaimers is enhanced by the message labeling system called message classification.

InstantDoc ID 102849

**William Lefkovics**
(william@mojavemediagroup.com) is a technical writer specializing in messaging and collaboration solutions and is technical director of Mojave Media Group in Las Vegas. He is an MCSE and a Microsoft Exchange MVP.

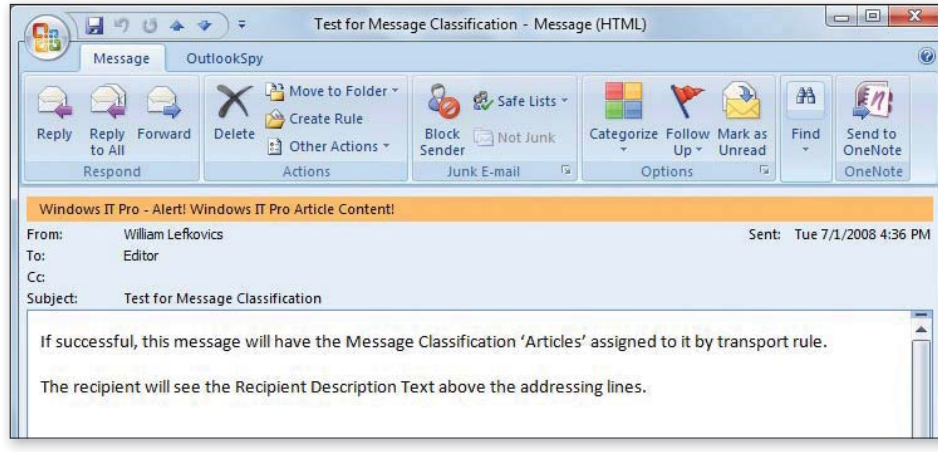



Figure 6: An email message with Recipient Description text displayed

# TIME TO ROUND UP THOSE SCRIPTS

by Jim Turner

## Don't leave your scripts scattered about on your computer

I have to admit that after many years of scripting I have scripts all over the place on my computer. They're in a variety of folders on different drives. Some are well organized, and some are not. Some I forgot about, while others have been hiding out in inconspicuous locations for a very long time.

To make matters worse, PCs aren't backed up where I work. Needless to say, if I were to have a disk go bad and lose all my scripts, I would be quite upset.

Instead of trying to hunt down all my scripts and copy them to a USB drive or a network location that is backed up, I decided to round them all up with a script. ScriptRoundUp.vbs uses Windows Management Instrumentation (WMI) to find all the .vbs and .hta files on my local C and D drives. The query used in the script can easily be modified to look at different local drives and to look for other file extensions, so you could round up Windows PowerShell scripts, Microsoft Word documents, or Microsoft Excel spreadsheets by making just a slight modification. Let's look at how to use ScriptRoundUp.vbs and how it works.

### How to Use the Script

Locating files using WMI is nothing new to most script writers, so what sets ScriptRoundUp.vbs apart from the many WMI scripts that you might already have? The main difference is that ScriptRoundUp.vbs makes copies of all the files meeting the specified criteria and places those copies in a centralized location so that you have all your scripts in one location. You can then copy them from the centralized location to a USB drive or network location in one fell swoop. This centralized location is hardcoded in the script as C:\Scripts\AllScripts\ScriptFiles. The script doesn't create this folder, so you must create it prior to running the script.

If you want to store the copies in a different folder, you just need to find the code

```
ColPath = "C:\Scripts\AllScripts\"
DestRoot = ColPath & "ScriptFiles"
```

near the beginning of ScriptRoundUp.vbs. (You can download this script by going to www.windowsitpro.com, entering 102139 in the InstantDoc ID box, clicking Go, then clicking the *Download the Code Here* button.) ColPath is the collection path where the script creates and stores an .xml database that contains information about all the files returned by the WMI query. In this case, the C:\Scripts\AllScripts folder contains the .xml database. DestRoot

specifies the destination root folder where all the scripts will be stored—in this case, it's the ScriptFiles folder. You can change this subfolder by modifying the second line, but be sure to leave the variable names ColPath and DestRoot intact. Once again, you need to create the subfolder before running the script.

VBScript files and HTML Applications (HTAs) usually don't take up a lot of space. (I have well over a thousand scripts and HTAs and they consume only about 56MB total.) However, if your C drive is extremely low on disk space, you might want to change the ColPath value to another folder location on a different drive.

The only other code you might want to modify is the WMI query

```
strQuery = _
  "Select Drive,Name," & _
  "Extension,Path from " & _
  "CIM_DataFile " & _
  "Where (Drive='c:' OR " & _
  "Drive='d:') AND " & _
  "(extension='vbs' OR " & _
  "extension='hta')"
```

This query looks for VBScript and HTA files on the C and D drives. You can easily modify this code to look for different types of files on different local drives. For example, if you want to find JScript and PowerShell files, you'd modify the statement to look like

```
strQuery = _
  "Select Drive,Name," & _
  "Extension,Path from " & _
  "CIM_DataFile " & _
  "Where (Drive='c:' OR " & _
  "Drive='d:') AND " & _
  "(extension='js' OR " & _
  "extension='ps1')"
```

After running the script (which could take a while, depending on how many scripts you have), open the destination root folder. You should find a folder for each of the hard drives listed in the query. If you open these folders, you should see a myriad of subfolders that contain your VBScript scripts and HTAs.

Before running ScriptRoundUp.vbs a second time, I suggest that you delete all the files and folders from the C:\Scripts\AllScripts folder after you've copied them to a safe place. If you leave them on your hard drive and run the script again, you'll end up collecting those files as well, virtually doubling the time it takes to run the script and doubling the amount of space used to house the files.

**Listing 1: ScriptRoundUp.vbs**

```
Const adPersistXML  = 1
Const adFldIsNullable = 32
Const adLongVarChar = 201
ColPath = "C:\Scripts\AllScripts\"
DestRoot = ColPath & "ScriptFiles"

strQuery = "Select Drive,Extension,Name,Path from CIM_DataFile " & _
  "Where (Drive='c:' OR Drive='d:') AND (extension='vbs' OR extension='hta')"

Set fso = CreateObject("Scripting.FileSystemObject")
If Not fso.FolderExists(ColPath) Or Not fso.folderExists(DestRoot) Then
  Msgbox "Collection Folder " & ColPath & " or " & DestRoot & _
  " does not exist... Terminating Script"
  WScript.Quit
End If

strMessage = "A message box will appear when process is complete."
strMsgTitle = "Script Round-up"
CreateObject("WScript.Shell").Popup strMessage,10,strMsgTitle,vbInformation

(A) Set objShell = CreateObject("Shell.Application")
Set RootFolder = objShell.NameSpace(DestRoot)

(B) Set DRS = CreateObject("ADODB.Recordset")
DRS.Fields.Append "Drive",adLongVarChar,256,adFldIsNullable
DRS.Fields.Append "Extension",adLongVarChar,256,adFldIsNullable
DRS.Fields.Append "Name",adLongVarChar,256,adFldIsNullable
DRS.Fields.Append "Path",adLongVarChar,256,adFldIsNullable
DRS.Open

(C) Set objWMIService = GetObject("winmgmts:" _
  & "{impersonationLevel=impersonate}!\\.\root\cimv2")
Set colFiles = objWMIService.ExecQuery(strQuery)
For Each objFile In colFiles
  DRS.AddNew
  DRS("Drive") = objFile.Drive
  DRS("Extension") = objFile.Extension
  DRS("Name") = objFile.Name
  DRS("Path") = objFile.Path
Next
DRS.MoveFirst

(D) Do While Not DRS.EOF
  FolderPath = Replace(DRS.Fields.Item("Drive"),":","") & DRS.Fields.Item("Path")
  Dest = DestRoot & "\" & Replace(DRS.Fields.Item("Drive"),":","") & _
    DRS.Fields.Item("Path")
  If Not fso.FolderExists(Dest) Then
    RootFolder.NewFolder(FolderPath)
  End If
  Set sourcefile = nothing
  Set sourcefile = fso.getFile(DRS.Fields.Item("Name"))
  sourcefile.Copy Dest
  DRS.MoveNext
Loop

If fso.FileExists(ColPath & "Scripts.xml") Then
  fso.DeleteFile(ColPath & "Scripts.xml")
End If

DRS.Save ColPath & "Scripts.xml",adPersistXML
DRS.Close
MsgBox "Done"
```

I should also point out that I chose to use a database as an interim holding tank because using a database makes the process much cleaner than copying files directly from WMI collections. Plus, if I decide to extend this script's functionality (e.g., have it look for duplicate files), I would have a means to do so.

## How the Script Works

As Listing 1 shows, ScriptRoundUp.vbs is relatively short and not too complex. I'll describe how it works, summarizing certain sections and elaborating on a few areas.

After setting up the reference variables and query string, the script checks to make sure both the C:\Scripts\AllScripts and C:\Scripts\AllScripts\ScriptFiles folders exist. If they don't, a message lets you know that one or both folders are missing and the script terminates.

Next, at callout A in Listing 1, ScriptRoundUp.vbs creates a Folder object named RootFolder that's bound to the destination root folder. (This object is part of the Windows Shell API for scripting.) Using the Folder object's NewFolder method, the script adds subfolders to the destination root folder. The subfolder names are derived from the actual folder names that house the .vbs and .hta files.

At callout B, the script sets up an ActiveX Data Objects (ADO) database to store the file information returned by the WMI query. The database is composed of four fields, each relating to specific WMI properties:

- The Drive field, which contains the file's drive letter (e.g., C)
- The Extension field, which contains the filename extension (e.g., vbs)
- The Name field, which contains the complete path and filename (e.g., C:\Scripts\RoundUp\ScriptRoundup.vbs)
- The Path field, which contains just the path with leading and ending backslashes (e.g., \Scripts\RoundUp\)

Shortly, you'll see how these four fields play an important part in constructing the subfolder names and copying the files.

In callout C, ScriptRoundUp.vbs executes the WMI query. The script stores the files that meet the criteria in a collection. A VBScript For Each…Next statement cycles through the collection. Each file's drive, extension, name, and path are retrieved and stored in the appropriate fields in the database. After all the file information has been added to the database, the record pointer is positioned at the first record.

The Do…Loop statement in callout D is the heart of the script—it's where all the subfolders get created and all the files get copied. Keep in mind that the subfolders are all created in the destination root folder. So, for example, the C:\Scripts\RoundUp\ScriptRoundup.vbs file would be copied to C:\Scripts\AllScripts\ScriptFiles\C\Scripts\RoundUp\ScriptRoundup.vbs.

Let's take a close look at the Do…Loop statement. The code

```
FolderPath = Replace _
  (DRS.Fields.Item("Drive"),":","") _
  & DRS.Fields.Item("Path")
```

**Backing up all your .vbs and .hta files is as easy as running ScriptRoundUp.vbs and copying the rounded-up files to your backup location.**

constructs the FolderPath variable's value from the drive letter (with the colon stripped out) and the path. The resulting value would look something like C\Scripts\RoundUp\. The FolderPath variable will be used to create the subfolder to house the file. However, before that occurs, the script tests for the existence of the subfolder in FolderPath. That way, if it already exists, an attempt won't be made to create it again. The code

```
Dest = DestRoot & "\" & Replace _
  (DRS.Fields.Item("Drive"),":","") _
  & DRS.Fields.Item("Path")
```

sets the Dest variable, which is used for the existence test. The Dest variable's value is created basically the same way as the FolderPath variable's value, except the Dest variable's value is preceded with the value in the DestRoot variable (i.e., C:\Scripts\AllScripts\ScriptFiles) and would look something like C:\Scripts\AllScripts\ScriptFiles\C\Scripts\RoundUp\.

After the Dest variable is set, the existence test takes place using the code

```
If Not fso.FolderExists(Dest) Then
  RootFolder.NewFolder(FolderPath)
End If
```

If the subfolder doesn't exist, the statement *RootFolder.NewFolder(FolderPath)* uses the name stored in the FolderPath variable to create the subfolder under the destination root folder.

Next, the lines

```
Set sourcefile = nothing
Set sourcefile = _
  fso.getFile(DRS.Fields.Item("Name"))
sourcefile.Copy Dest
```

disassociate the sourcefile variable with any object, then set that variable to a Scripting Runtime Library File object that's bound to the file associated with the value stored in the Name field of the database. Remember that the Name field contains the full path and filename of the file that was initially returned by the WMI query. With the File object created, it's simply a matter of calling that object's Copy method to copy the .vbs or .hta file specified in the Name field into the subfolder specified in the Dest variable. This process is repeated for each record in the database until reaching the end of file (EOF), after which the database is saved as C:\Scripts\AllScripts\Scripts.xml.

That's it! All you have to do now is copy the files that you rounded up to wherever you want. Don't forget to delete them from the collection area if you plan on running the script again using the same criteria.

InstantDoc ID 102139

**Jim Turner**
(jturnervbs@gmail.com) is a domain administrator and applications developer for Computer Sciences Corporation.

# Spicing Up SharePoint Search Results

by Ryan Thomas

Combining out-of-the-box tools with third-party and custom solutions can help you build your way to a sleeker, more powerful SharePoint environment

A significant number of organizations that use Microsoft Office SharePoint Server (MOSS) are failing to leverage some easy ways to improve both the quality of their data and the quality of their search results and associated user experience.

Companies typically face common SharePoint search problems when they attempt to implement useful metadata options and quick and easy customizations. Others are constantly seeking small ways to move their intranets, collaboration data, and portals in the right direction for growth and maintenance. I want to provide help in those directions. I won't promise a huge lesson in enterprise information architecture or any grand scheme for overhauling the governance of your data or SharePoint environment, but I can suggest a number of free/inexpensive tools and useful ideas to help you improve the structure and content of your data.

## The Problem

The most common scenario I see among SharePoint-using clients is a lack of design and planning at the data level. Many organizations have spent considerable time and IT dollars building a hardware and farm infrastructure, but they've spent little or no time working on the design of the actual data. A significant number of these implementations include a Help desk, site-provisioning tools, custom site definitions and templates, and a formal process for managing the farm, but they don't have a single custom content type, and during the analysis and design phase they haven't created any customized search results. Site administrators typically let the site owners use the available out-of-the-box SharePoint tools to organize their own data. This approach leads to either very little data management or inconsistent architecture and design across sites and search results.

The problem increases over time as users add, version, and collaborate on larger and larger amounts of data in sites that have little or no metadata or classification. Users continue to upload documents into the pile and rely on SharePoint's search engine to index content and properly return results. Eventually, this system breaks down when the volume of documents becomes so large that search results are significantly littered with correct but unintended results. SharePoint's out-of-the-box search cries out for some options to filter the data into usable compartments. These filters can be standard metadata items such as the author, content type, and language; however, additional options available via search scopes and limitations based on location or custom properties can greatly increase relevancy.

IT pros within the organization face a daily challenge. They generally need to understand enough about all the disparate data sources within the corporate firewall to locate pertinent information to complete their job functions. They often ask to search for multiple locations in a single location instead of logging on to remote applications or websites and searching and tallying results manually. They want more options to sort and drill down on the data returned. They also might need to manage the data, either by asking for and receiving additional metadata within their results, gaining access


# HARNESS THE POWER OF VIRTUALIZATION FOR YOUR BUSINESS.

The IBM® System x3550 M2 Express, powered by the Intel® Xeon® processor 5500 series, is one of the industry's leading x86 servers for virtualization. With its Integrated Management Module, you can easily manage, monitor and troubleshoot your physical and virtual servers locally and remotely. Allowing you to reduce the cost of managing your IT.

IBM express advantage™

## IBM SYSTEM x3550 M2 EXPRESS

**$2,589**

OR $67/MONTH FOR 36 MONTHS[1]

PN: 7964-E2U

Featuring up to 2 Intel® Xeon® processor 5500 series

Energy-efficient design incorporating low 675 W and 92% efficient PS, 6 cooling fans, altimeter.

## VMware® vSphere™ 4.0 ESSENTIALS KIT

License, Subscription and Support required

License Only: VMware vSphere 4.0 Essentials Kit, 3-2 Socket Hosts, PN: 4817VA8 $879

Subscription Only: VMware vSphere 4.0 Essentials Kit – 3-2 Socket Hosts, PN: 4817SA8 – 1 year, $119

VMware RTS: 1-year support, PN: 51J8632 $284

## IBM SYSTEM STORAGE™ DS3200 EXPRESS

**$4,495**

OR $116/MONTH FOR 36 MONTHS[1]

PN: 172621X

External Disk Storage with 4 Gbps Fibre Channel interface technology

Scalable to 3.6 TB of storage capacity with 300 GB hot-swappable SAS HDDs or up to 9 TB of storage capacity with 750 GB hot-swappable SATA HDDs

**LEARN MORE**
about the benefits of virtualization with IBM and VMware

**ibm.com/systems/virtualize**
**866-872-3902** (mention 6N8AH20A)

[1]IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on a FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. VMware and vSphere are registered trademarks of VMware, Inc. www.vmware.com. IBM, the IBM logo, IBM Express Advantage, System Storage and System x are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. All other products may be trademarks or registered trademarks of their respective companies. All prices and savings estimates are subject to change without notice, may vary according to configuration, are based upon IBM's estimated retail selling prices as of 7/1/09 and may not include storage, hard drive, operating system or other features. Reseller prices and savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Prices are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area. 

to custom search applications, or modifying components of the actual data as required and allowed.

## Start with Legwork

You need to realize that it's almost impossible in a large organization to perform a complete analysis and formulate a master plan in advance. Convincing budget makers, stakeholders, users, and a committee to take on months of meetings and design sessions is generally unattainable. The risk starts to become too visible. Although the rewards can seem empowering, they can also be very difficult to achieve. My opinion is that a waterfall approach to this process is a setup for failure.

Instead, I recommend tackling the first small problem you want to solve. Such problems will be different for each department and user, but you're probably considering this project because you're already aware of a few data, organizational, or search concerns based on community complaints. Those with the loudest complaint will be the most likely to help formulate a solution, creating the perfect opportunity to start solving specific, incremental problems.

This article is about tools and options for correcting such problems, but you need to understand the importance of advance legwork. Forming a small committee of decision makers and users willing to meet quickly every week can be beneficial. This group can help communicate requirements from different aspects of the organization and can evaluate potential tools and solutions in a testing environment. Those involved also serve to evangelize your options within the organization—key to getting the word out about any changes and to soliciting feedback.

Before we jump into your options, remember to stay focused without losing sight of the big picture. Keep your cycles short, and get some small wins, but understand that each small win adds another component to your overall solution. You'll gradually gain knowledge about the data in your organization while also solving specific problems. With proper attention to the big picture, you should end up with a relatively stable solution and a significant understanding of how your architecture is pieced together (as well as what gaps remain).

## Out-of-the-Box Options

Let's begin with basic options available to everyone using at least MOSS. Following are simple descriptions of the options and how you can use them.

***Content Sources.*** Content Sources denote the items that SharePoint's crawling engine looks at and creates a searchable index for. Keep in mind, these can be broken out for scheduling and different rules, even among internal SharePoint locations, helping with time management and handling large data stores.

***Managed Properties.*** Managed Properties are the metadata items that the crawling engine finds when viewing your data. They even pick up custom columns in SharePoint lists. You can roll these up into custom properties and use them as rules and filters in search scopes and advanced searching techniques.

***Search Scopes.*** You can configure SharePoint to limit the scope of a search by managed property (equal or not equal to), by locations, and by content class. The content class is a little-known property in SharePoint that represents an item's internal classification—for example, List Type and Item Type. You can use these properties to create scopes that will return only web pages instead of list items or documents. A significant number of other classification options are also available.

***Thesaurus.*** Many administrators aren't aware of the SharePoint thesaurus, a system-level XML file that lets you create global replacements for common terms. This feature removes the burden on site-collection administrators of creating custom keywords for each new site collection when common domain-level terms need to have synonyms in their searches.

***Keywords and Best Bets.*** Critical and often overlooked, these items give the individual site collection the power to create keywords with any number of synonyms as a search replacement. The real benefit is the ability to create Best Bets, which let users add links to any content that will automatically appear at the top of search results when a keyword or synonym appears in the search terms.

***Custom search pages.*** The makeup of the standard Search Results page has a significant number of web parts that represent a large number of options for the end user. I'll discuss just the core Search Results web part. This web part is essentially just a large Extensible Stylesheet Language (XSL) transform code block. It takes the Extensible Markup Language (XML) search results and transforms it to whatever you, the end user, and designer put in place.

One of the best ways to evaluate your options is to look at the raw XML returned from your search to see what data is actually available for designing a custom search page. You'll see that many properties are included—specifically, the custom properties you've defined in your Shared Services Provider (SSP). This step lets you include additional data, group the data and add custom links based on If statements, and so on. Depending on the type of data you expect to return in your results, you can create very specific views of this data.

Understand that you aren't limited to the single Search Results page offered by SharePoint's out-of-the-box search center. You can create as many custom pages as you want, with very specific criteria and results layouts. Simply linking to them from appropriate locations within your organization can direct people to more focused search locations.

## Third-Party or In-House Tool Options

Although there are many additional out-of-the-box enterprise search-management approaches, you need to be aware of additional tools and third-party components. The following tools are in no particular order, and many are open-source.

***User ratings.*** With the advancement of Web 2.0—and its focus on socialization, networking, and data-interaction freedom—SharePoint content needs a boost to handle some of the requirements of this new environment. Thankfully, SharePoint is an easy platform to work with from a development perspective, and there are some free and inexpensive third-party web solutions that can do most of the work for you.

Rating content has become crucial to the interactive style of modern technical communication. Not all enterprise data needs or warrants rating from the user community, but a large amount does. You can download and install functionality to provide a common star-rating column for any SharePoint list or library. The tools are intelligent enough to permit only a single rating by each user

account, and they also support comments. Site owners can add this feature to only the lists and libraries they choose. The ratings are simple and easy to add to search results pages, with filtering based on minimum star rating.

***Facets.*** There are free, open-source tools available that allow dynamic pivoting on properties returned in the Search Results XML file. You can customize the tools to add or limit the specific properties that are available for pivoting in each search result. They are 100 percent UI-based, letting you select links to continue drilling down and filtering on as many properties as you want. The software shows you which filters you've applied and lets you remove them individually at any time. You can add these web parts to any Search Results page.

SharePoint is an easy platform to work with from a development perspective.

***Federation.*** In the summer of 2008, Microsoft released its Infrastructure Update for MOSS, which included the ability to call external (or internal) search locations and return the results to a web part. You can use almost any search engine to run queries in real time and return the results to SharePoint. This becomes a powerful tool when you're creating single-location search centers that can simultaneously search all internal search engines and return the results from a single query. With Federation, you can even search SharePoint search scopes specifically by using a federated location, thus querying multiple SharePoint search scopes in a single query but segmenting their results into usable buckets. These federated search web parts can also search external search engines if you need to include results from public locations. (Be aware that your users will be broadcasting search terms to public locations.)

***Export data into SharePoint.*** Although this capability might seem backwards from a search perspective, consider exporting data from other line-of-business applications into HTML pages and importing them into SharePoint at regular intervals. Think about some potential wins: Owners of other applications get to choose what data to query and export, they can design a metadata scheme to apply to their data as it's imported into SharePoint, they choose the intervals at which data is exported, and they control the layout and structure of how their data is viewed. Using some of the SharePoint web services or relatively simple programming can accomplish the import tasks. Therefore, SharePoint can have native content added to lists and libraries and crawl it as local content instead of using the Business Data Catalog or Federated Search to query external data held within other applications.

***Custom web parts.*** With four or five days of development, you can build a custom web part that queries an internal database, looks up metadata for common document details within your organization, and uploads a document with routing rules. If you have proprietary business data that would be beneficial to apply as metadata to SharePoint documents, a custom tool can be powerful. Essentially, the project queries other internal databases to look up pertinent data that you want to apply to documents being uploaded to SharePoint. With some basic business logic, this web part can look up linked data based on user selections, then upload and route the document based on the applied metadata. This solution lets you apply important properties to your SharePoint content without requiring your users to enter all the data by hand.

***BDC.*** Although entire books have been written about the Business Data Catalog (BDC), it's worth mentioning the power that it can hold from a data-querying and data-retrieval perspective. The BDC data can be quite interactive and used in various web parts, can connect to other web parts for filtering, and can be added to lists as custom columns. Ultimately, it can be read in a very similar fashion to list data in SharePoint. What we care about is how it can be searched. The BDC can connect to internal applications that can be accessed via an ADO.NET provider or web services. Data can be set up as a content source in SharePoint (Enterprise version) for crawling and indexing and can then be searched and returned via standard SharePoint searching capabilities. This can all be done without coding, yet a significant amount of XML must be written. A few excellent tools in the marketplace can help you create these XML definition files.

## Available Tools

I want to call out some tools that are available as free downloads. Most of the options I outlined are available in some form at CodePlex (www.codeplex.com). There are various versions, each with strengths and weaknesses. I encourage you to set up a test environment and test them. The site contains almost all the tools and utilities you'll need to help with search; I use them regularly. Here are some additional items and ideas to consider:

- Viewing tool—This tool lets you load and view all your SharePoint sites from a tree view, starting at a web application and drilling down to properties on a list item.
- Search tool—This tool lets you query the engine directly via an external UI.
- Tool for modifying relevancy rankings and testing the results.
- XSL samples from other people in the community—These can show you what others are building for search results pages.
- Adding wildcard searching options.
- Better management of searches based on custom properties.
- Regular Expression searching tools—These let you create custom regular expressions to search content in SharePoint. They're ideal for uncovering specific formats of data, such as credit card numbers, telephone numbers, and social security numbers.

Hopefully, some of these ideas will empower you and your organization to begin making changes to help improve and spice up your SharePoint search results. Happy searching!

InstantDoc ID 102755

**Ryan Thomas**
(rthomas@syrinx.com) is director of the SharePoint Practice at Syrinx Consulting. He's a Microsoft Certified Professional Developer and Microsoft Certified Application Developer, and contributes regularly to the Syrinx SharePoint blog and other industry publications.

## Kace and Bomgar Announce Partnership

Systems management appliance vendor Kace Systems and remote support specialist Bomgar announced that they've inked a partnership deal. Under the terms of the agreement, Kace customers using a Kbox appliance will be able to access Bomgar's remote support products from within the Kbox management console. "Our partnership with Bomgar is derived from a common vision—bringing innovative and robust appliance-based technology to market, which can be easily deployed and used by organizations of all sizes yielding unparalleled investment return rates," said Marty Kacin, president, CTO and co-founder of Kace in a statement announcing the partnership news. "Through this partnership, we continue to expand the suite of automation and security solutions available to our customers—providing them unmatched systems management and remote desktop control capability, all delivered within the industry's most innovative stack of appliance offerings." For more information, visit www.kace.com or www.bomgar.com.


## PRODUCT SPOTLIGHT

### Remote Administration Software Puts a GUI Face on WMI's Functionality

With PJ Technologies' **WMIX 2.0,** you don't have to know how to write scripts to take advantage of Windows Management Instrumentation's (WMI's) functionality. WMIX is a GUI-based implementation of WMI. Because it has a GUI, anyone can query and manage remote Windows machines—no scripting is necessary. Because it's based on WMI, you don't have to install any software agents on the client machines.

With WMIX, you can perform such tasks as querying and configuring settings and executing management tasks on local and remote machines. You can also generate built-in or custom reports. The enhancements in version 2.0 include a built-in script generator and a WQL query wizard. The built-in script generator lets you automatically generate a script for any task you initiate using the GUI. The generated scripts are automatically configured so that they can be run against the local machine, a remote machine, or a group of machines. In addition, all WMI parameters and values are converted to a user-friendly format.

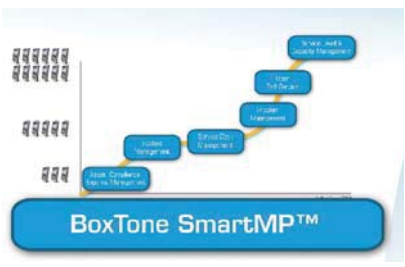
Using WMI Query Language (WQL) queries to filter information that WMI returns is very helpful. However, creating WQL queries can be difficult because you need to know about WMI class definitions and WQL's syntax. WMIX includes a query wizard that guides you through the process of creating WQL queries.

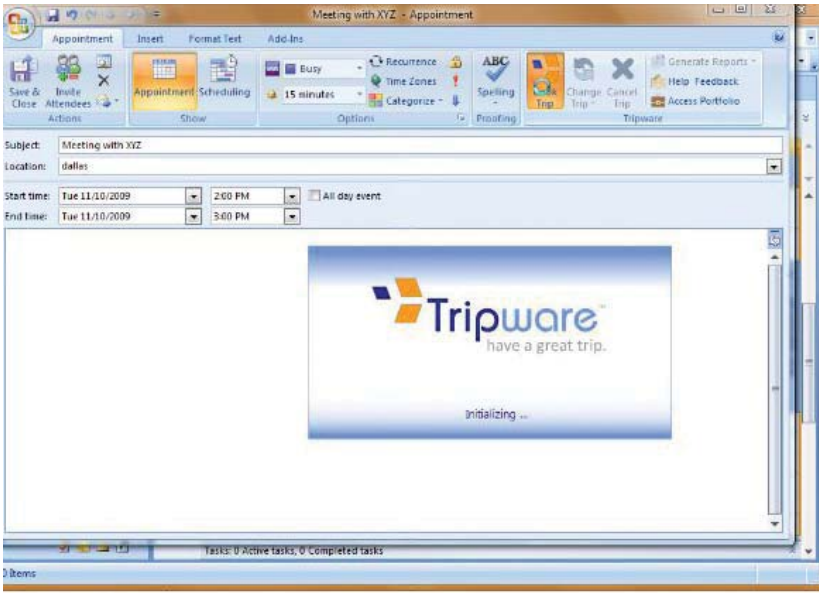
WMIX 2.0 runs on Windows 2000 and later, and supports clients running Windows NT SP3 and later. It's priced at $89 per user license. For more information, visit wmix.pjtec.com or contact PJ Technologies at sales@pjtec.com or 786-268-3517.

Brian Reinholz | breinholz@windowsitpro.com
Editor's Note: Send new product announcements to products@windowsitpro.com.

## BlackBerry User Self-Service Eases Help Desk Burden

BoxTone's new module—called **User Self-Service**—allows users to quickly, easily troubleshoot their own problems without training and without the Help Desk, reducing Help Desk calls by 30-50 percent, according to the vendor. Since most of an organization's BlackBerry users are VIPs that can't tolerate or afford downtime, user self-service is a good model for improving employee satisfaction and efficiency. One limitation to this product is that users need to be able to access the web in order to troubleshoot their device. BoxTone's solution is sold in modules, meaning you can point and pick the services that you want, pay for what you order, and then upgrade or alter it later if you need to (User Self-Service is one such model). A deployment with 1-2 modules, on average, runs at about $35/user. To learn more, call 410-910-3344 or visit www.boxtone.com.






## Tripware Books Travel Directly in Microsoft Outlook

**Tripware** is a travel tool that allows users to plan, book, and manage their travel needs and business meetings with one tool, profile, and itinerary in Microsoft Outlook 2007. To use Tripware, you create a meeting in Outlook, then click 'Book Trip' and set preferred destination/arrival, whether you want a car rental or hotel, etc., and then have Tripware give you a preferred flight, rental, etc. Tripware also analyzes habitual and repetitive behaviors to further automate the process, so if you always stay at the same hotel chain, for instance, it will give you that chain if you want by default. Tripware runs off of the .Net framework and is the only Microsoft Office plug-in that books travel, according to the vendor. To download the free plug-in, visit www.tripware.com.

## Bluelounge presents Refresh

Bluelounge introduces **Refresh,** a charging station that allows you to charge four devices simultaneously. Compatible with over 1,000 products, it comes with the following six connectors: two iPod/iPhone connectors, a Micro USB, a Mini USB, and two USB Sockets. The charging station is compatible with the following brands: Apple, Blackberry, Creative, Dopod, Eten, Garmin, HP, HTC, i-mate, Insignia, Iqua, iRiver, Jabra, LG, Memorex, Motorolla, Noki, O2, Pal, Philips, Plaantronics, Qtek, Samsung, Sanyo, Sidekick, Sony and Toshiba. Bluelounge Refresh is offered in white, black, and pink and retails for $89.95. It is also available through www.bluelounge.com.


# Paul's Picks

www.winsupersite.com

**SUMMARIES** of in-depth product reviews on Paul Thurrott's SuperSite for Windows

### Microsoft's Cloud Computing Strategy

**PROS:** A surprisingly cohesive migration strategy for positioning Microsoft as a provider of cloud-based services.

**CONS:** Partners are cut out when Microsoft hosts its own solutions.

**RATING:** ◆◆◆◆◇

**RECOMMENDATION:** As its future revenue streams from desktop products dry up and its server products move from on-premises to hosted subscription services, Microsoft needs to profit from cloud computing. Compared to pure cloud-based companies like Google, it has two advantages: decades of experience and millions of customers, and a hybrid strategy that will prove invaluable to its most important customers: the enterprise.

**CONTACT:** Microsoft • 800-426-9400 • www.microsoft.com

**DISCUSSION:** www.winsupersite.com/server/fam_2009.asp

### Apple Mac OS X "Snow Leopard"

**PROS:** Mature, capable OS, excellent performance, free Exchange interoperability.

**CONS:** No major improvements, doesn't change the "switcher" value proposition, works only with latest Exchange version.

**RATING:** ◆◆◆◆◇

**RECOMMENDATION:** Mac OS X 10.6 "Snow Leopard" is a nice refinement to an already solid OS. But we'd call it a service pack in the Microsoft world—and it certainly doesn't offer incentives to switch. Comparing Snow Leopard to Windows 7, Microsoft's is the more substantial offering, providing internal updates just like Snow Leopard but also major updates for users. Still, Apple made some nice performance improvements, getting set for further innovation.

**CONTACT:** Apple • www.apple.com

**DISCUSSION:** www.winsupersite.com/alt/snowleopard.asp

InstantDoc ID 102826

# Axceler ControlPoint

Many IT pros have rushed to deploy SharePoint. The result is a proliferation of SharePoint installations that busy IT pros have to manage. Some management tools are included with SharePoint, but for now those management tools are somewhat limited. As the footprint of your SharePoint deployment grows, you need better tools to help you control it. We'll take a look at one product that promises to help you manage your growing SharePoint infrastructure: **Axceler ControlPoint**.

## A Control Point for SharePoint

The Axceler website bills ControlPoint as a management tool that lets you "explore, protect, analyze and control your SharePoint environment." Axceler goes about that by bolstering the native capabilities of SharePoint in the areas of governance policy enforcement, content management, permissions management, and the ability to easily move sites and site collections.

Installing ControlPoint was straightforward, and it includes options for deploying the tool to single farm or multi-farm SharePoint deployments. ControlPoint runs as a web app that is much like your SharePoint operations page, but with many more features.

## Moving Sites and Site Collections

Some of my favorite ControlPoint tools deal with moving sites and site collections. From an admin's view the ability to move sites and groups of sites from one site collection to another is very helpful, and moving them from farm to farm is a task that ControlPoint can really help with.

One common problem is that a SharePoint site user will have security problems with accessing parts of a site collection. ControlPoint provides tools to analyze the security problems and allow an admin to make a fast problem resolution. Administrators may often trust another IT pro to manage a SharePoint site collection, but granting large amounts of control can also create big problems. ControlPoint helps alleviate these problems by providing a robust alerting system that makes you aware of urgent issues like deleted sites or broken security inheritance.

Some companies will have documents that are extremely valuable, and compliance requirements may require a history to be kept of what the security settings have been since those documents were added to the document library. Out of the box, SharePoint doesn't provide a way to clone permissions from several site collections to a single user with just a few mouse clicks. ControlPoint lets you perform that procedure by using a duplicate user permissions process.

ControlPoint can generate comprehensive site reports that give managers and administrators information about all the users with access in a SharePoint farm and the content and data access levels they have.

An intuitive interface lets you navigate through SharePoint sites, lists, and users. ControlPoint's interface integrates well with SharePoint. I liked this integration because a new administrator can drill through the conventional SharePoint management screens, and rely on the ControlPoint power tools to perform operations on a critical SharePoint application. While the interface is helpful, ControlPoint isn't for novices: Some SharePoint knowledge is needed to realize the full potential of this product.

InstantDoc ID 102838

### Axceler ControlPoint

**PROS:** Has strong tools for managing large deployments; integrates well with existing SharePoint user interface; the ability to manage user permission levels is nicely implemented

**CONS:** Expensive for small deployments; requires some substantial SharePoint knowledge to really take advantage of the tools

**RATING:** ◆◆◆◆◇

**PRICE:** $10,000 for average SharePoint farm plus $2,000 per year for support

**RECOMMENDATION:** ControlPoint isn't for new SharePoint farms with a few users; the product is designed for larger SharePoint farms and provides the tools and intelligence to help you manage and monitor large farms effectively.

**CONTACT:** Axceler • www.axceler.com • 781-995-0063

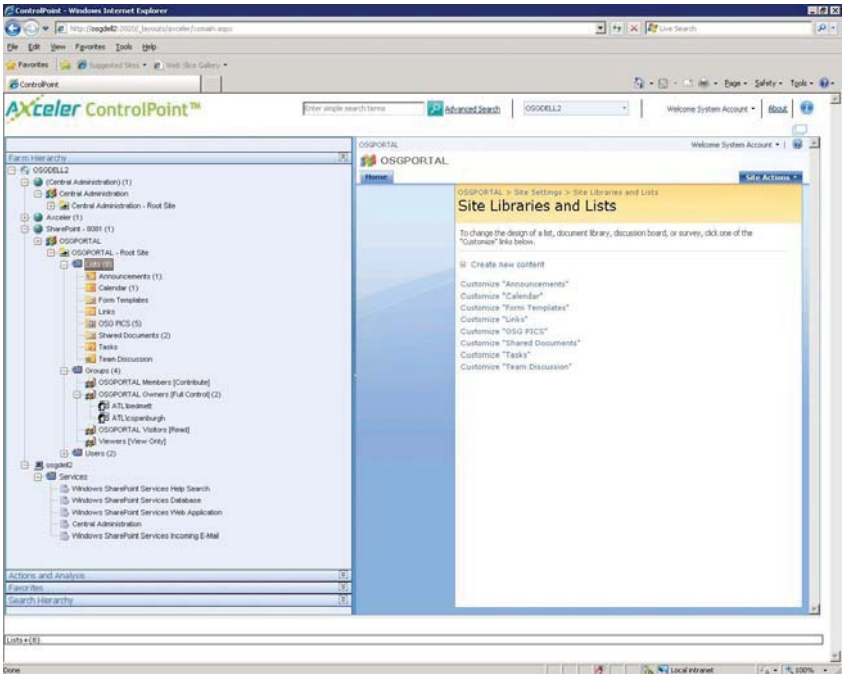



Figure 1: ControlPoint makes it easy to manage SharePoint site lists and libraries.

Curt Spanburgh (osgcurt@onesolutiongrp.com)

# Log Manager ROUNDUP

## Manage, monitor, and get more control over event logs

by Lance Whitney

Hunting through yet another Windows event log is often a necessary but time-consuming chore. One tool that can simplify this task is a Windows event log manager. An event log manager can help you more easily monitor and manage your event logs, find specific events, and generate reports.

### Taking 5 Log Managers for a Spin

For this log manager roundup, I looked at five different Windows log managers. Depending on your needs, any of these five products would be a good alternative to the standard Windows event viewer.

- FSPro Labs' Event Log Explorer
- Altair Technologies' Event Reader 2
- Dorian Software Creations' Event Analyst
- Technology Lighthouse's EventMeister
- Corner Bowl Software's Corner Bowl Log Manager 2009

All five products support the EVT format used by Windows Server 2003 and Windows XP to save event log files, but not all support the EVTX format, which Windows Vista and Windows Server 2008 use for event log files.

To test the log managers, I installed each one under Windows 2003 as my base OS. I also installed products compatible with Vista and Server 2008 under those two systems to confirm compatibility and make sure they could read EVTX files directly.

Of the five, the only program incompatible with Vista or Server 2008 was Event Reader 2. The company said that Event Reader 3 will support the newer OSs, though no release date was given.

Event Log Explorer, Event Analyst, Event Meister, and Corner Bowl Log Manager run on Windows Server 2008/Vista/2003/XP/2000/NT; Event Reader 2 runs under Windows 2003/XP/2000.

### Event Log Explorer 3.1

FSPro Labs' Event Log Explorer (see Figure 1, page 50) provides a no-frills window with a tree view of the computer on which you installed the program. You drill down on your current machine to see branches for each separate log file and double-click each log to open a list of its events in a table.

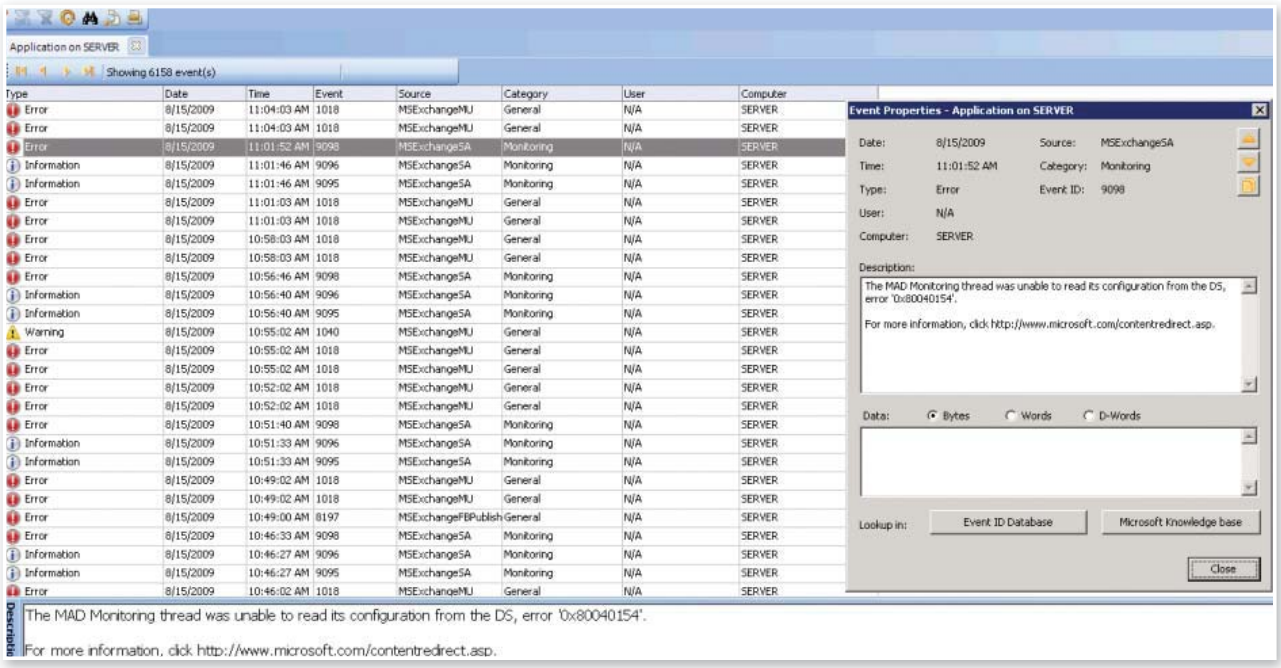



Figure 1: Event Log Explorer 3.1

Double-clicking a specific event opens a separate window consolidating information about the event type, date, time, and more. You can also find links to Microsoft's Knowledge Base and to the Event ID database, a web-based repository of Windows event log information.

From the UI, you can add other computers to the tree view. A wizard automatically scans for other computers based on their role on the network.

If you want to see just one specific log from another computer rather than all logs, you can run the Open Log command instead, browse the network or domain, then choose the machine. The Open Log File command lets you open existing EVT or EVTX log files from your local computer or any networked machine. To manage the many logs from different computers, you create multiple workspaces, each one storing a different tree of logs.

To sort the events displayed in the main window, you can click on any column heading. To narrow the events displayed, you can apply filters by running the Filter command. The filtering system is very effective, offering a nicely-designed dialog box. You can save any filter and apply it to other logs.

A convenient Quick Filter option is also available to filter the log based on your current selection. To limit the number of events loaded, you can prefilter events before they open. You can also search through all the displayed events using the Find command.

Event Log Explorer lets you save any log as an EVT or EVTX file, so you can keep a running archive. The software offers both manual and automated processes for backing up.

You can export any log from Event Log Explorer into HTML to generate a report, or save it as a text file or Excel spreadsheet to incorporate into a database. You can choose to export all events or only selected ones, and include or exclude event descriptions, but nothing more. However, it doesn't include a scheduling feature, so you can't automatically generate a report and have it emailed.

### Event Log Explorer 3.1

**PROS:** Clean and simple UI; very effective filtering system

**CONS:** No option for report scheduling

**RATING:** ◆◆◆◆◇

**PRICE:** Free for personal use (can monitor up to three computers on a home network); starts at $99.95 to monitor up to five servers

**RECOMMENDATION:** Event Log Explorer is a simple, well-designed product, ideal for any IT admin with basic log management needs.

**CONTACT:** FSPro Labs • 7-0-903-438-4643 • www.eventlogxp.com

## Event Reader 2

Event Reader 2 from Altair Technologies (see Figure 2) displays a tree view of your local computer, and you can drill down to see branches for each of the individual event logs. Clicking on a specific log displays its events and event properties. An Event Properties window displays a description of the event you select and its individual properties. Clicking the Event ID for a specific event brings you to the Event ID database, the web-based resource started by and still maintained by Altair Technologies.

By default, Event Reader displays the logs for the computer on which it's installed. You can add additional computers to monitor. Event Reader 2 supports only EVT files, not EVTX.

You can easily sort the events in any list by clicking the heading for each column. Event Reader offers several useful options to filter your data. A toolbar across the top displays buttons for each of the different event types, such as error, warning, and information. By default, all the buttons are turned on, but you can also exclude each type from the display.

More advanced filtering options also are available, including filtering by event type, by date and time, and by event ID and source. The filter options were smoothly presented and simple to use. Event Reader offers no specific method to search for events. But in

most cases, filtering provides a more efficient way of seeing events based on specific criteria.

To create a report, you can export an event log into HTML. Event Reader provides a few basic but helpful options to format your HTML report, letting you choose the font, point size, and colors. You can also save a log directly to an FTP server, which simply uploads it as an HTML report. And you can export event log data to a database.

The scheduling feature is impressive. You can schedule a report to be generated daily or at other intervals. You can set up the report to be saved in a specific location, emailed to you, uploaded to an FTP server, saved in a database, or all of those options. To limit the information in the report, you simply set up a filter.

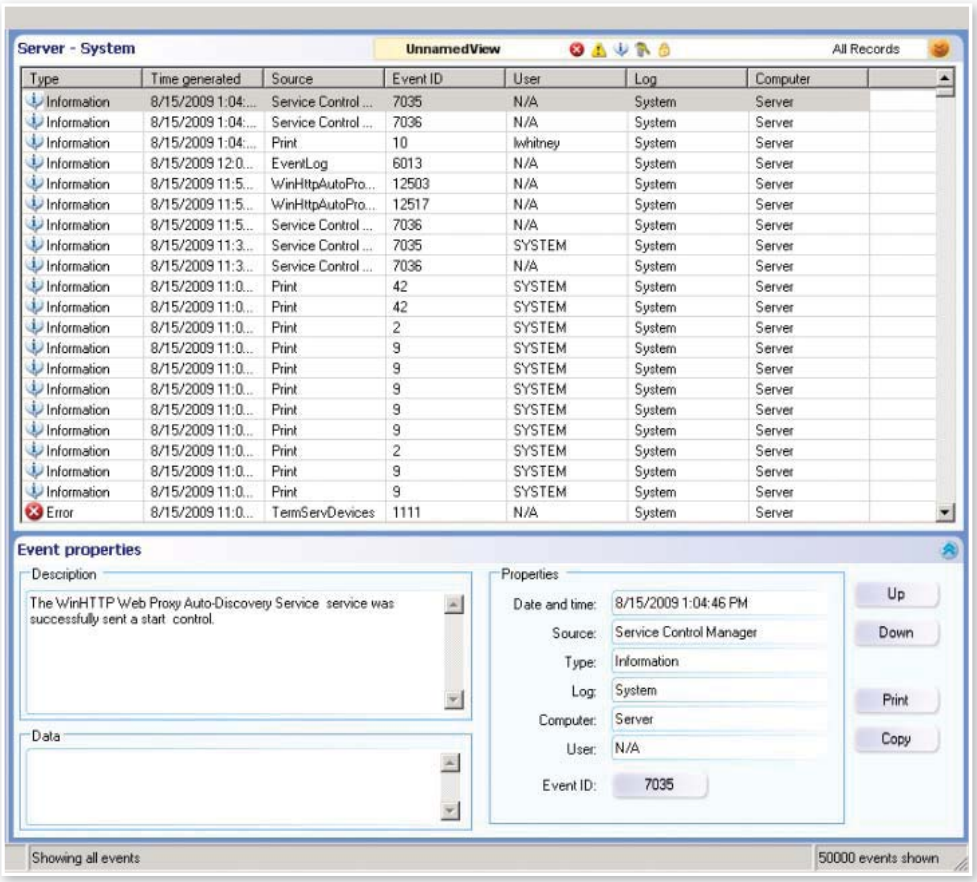



Figure 2: Event Reader 2

## Event Reader 2

**PROS:** Clean, simple interface; impressive report scheduling feature

**CONS:** Doesn't support Vista and Server 2008 because it can't read EVTX files

**RATING:** ◆◆◆◆◇

**PRICE:** Starts at $39

**RECOMMENDATION:** An inexpensive but solid piece of software, good for IT admins on a tight budget. If you don't need to support Vista or Server 2008, Event Reader is a smart choice.

**CONTACT:** Altair Technologies • 416-628-7295 • www.altairtech.ca

## Event Analyst 8.0

Event Analyst from Dorian Software Creations (see Figure 3) opens by greeting you with a Quick Tips message, which you can enable or disable at startup. After that, a blank UI awaits your command. When opening logs, you can choose only one computer and one log at a time; there's no option to tag multiple computers or logs to open in one shot.

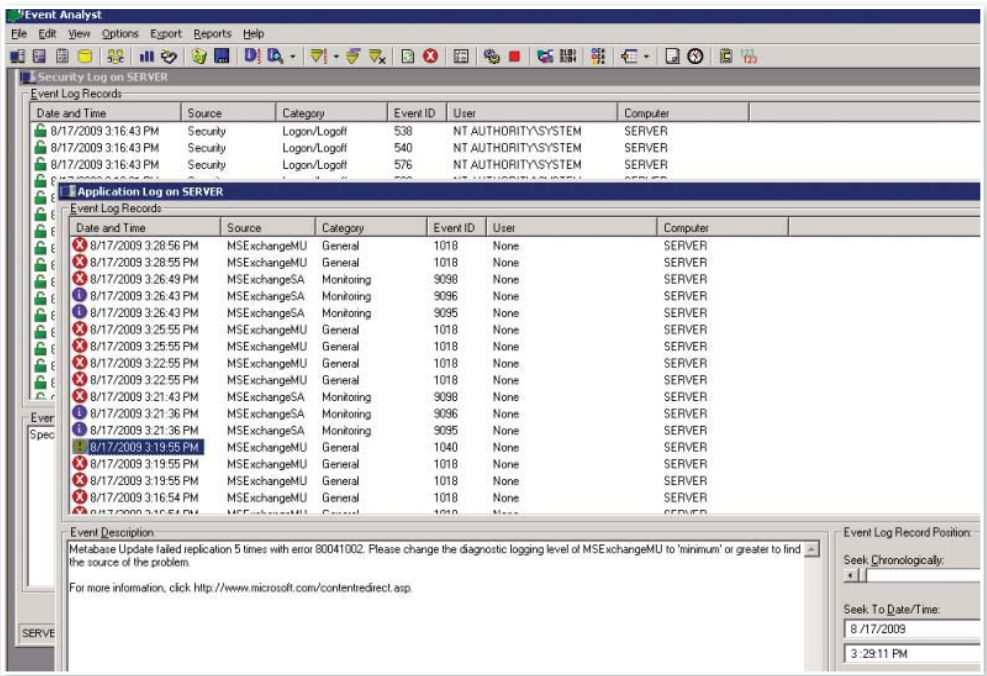



Figure 3: Event Analyst 8.0

You can tell the software to open the logs in the UI or build a report. You can add additional logs, either from the same computer or from other networked computers. You can also open files saved as EVT, EVTX, CSV,

or text to display within Event Analyst.

The Research this Event Online command opens a Dorian Software webpage with links to information on the event. You can also link to the Microsoft knowledge base.

You can sort the event list by any of the column headings. However, there was no heading for event type, so I wasn't able to sort the list to see all errors or all warnings grouped together.

Event Analyst includes several predefined filters to limit the event data on display. I created and saved a filter and was able to use it on any log by running the Apply Filter command. I could also create a basic filter on the spot without having to save it.

You can run an advanced filter that works against a database—Access, SQL Server, or Oracle. This method provides a wide range of options using Boolean logic to filter by computer, user, event ID, and other criteria.

Logs can be exported to any one of four formats: HTML, comma delimited text file, Access MDB file, or as ODBC source to a database. You can run a report based on specific criteria of your choice or choose a built-in report. Some of the built-in reports were extremely clever and useful, such as "Top 10 Most Frequently Occurring Events." Each report contained the source of the event and other details, along with the start and end dates.

Event Analyst's custom report designer proved quick and easy to use, and I was able to preview it as an HTML or CSV file. You can schedule a report to run on a regular basis and be saved or emailed. You can also apply a filter to the scheduled report to limit the amount of data it contains.

### Event Analyst 8.0

**PROS:** Well designed UI; clever built-in reports; easy-to-use custom report designer

**CONS:** Pricier than other log managers when you need to monitor multiple computers

**RATING:** ◆◆◆◆◇

**PRICE:** Separate server and workstation pricing: starts at $69.99 to monitor one server, $29.99 to monitor one workstation

**RECOMMENDATION:** Event Analyst is a solid and powerful product that's easy to use and manage.

**CONTACT:** Dorian Software Creations • 866-682-3646 • www.doriansoft.com

## EventMeister 3.0

Technology Lighthouse's EventMeister (see Figure 4) lets you set up a service to collect data when no user is logged in. Before viewing any log file data, you set up an Event Log Feed, which gathers events from the computers you want to monitor into one ongoing feed. You choose which event logs to include, how you want event information to be gathered, and how often to poll and update the feed with new data.

EventMeister uses either a "Read from log" option, which generates the feed by capturing all events from the log, including those stored before the application was installed; or it uses a "Catch events" option to capture new events, omitting older events. You can add new feeds from other computers to an existing group or create a new group and populate that with new feeds.

After the feed is created, the event log you chose is automatically downloaded. You can see a list of each event including such fields as type, date, and category.

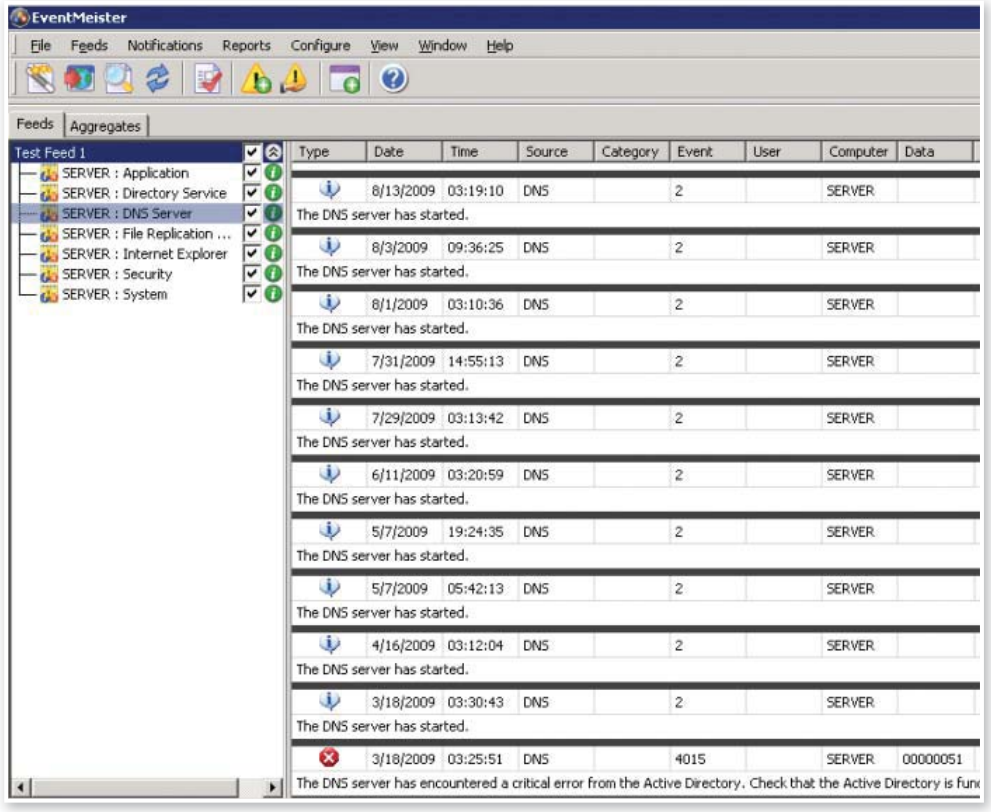



Figure 4: EventMeister 3.0

You can also create a feed by opening a CSV file. This is a useful option if you already have several feeds exported and saved into one single CSV file. However, there's no way to open an EVT or EVTX file directly. For this option to work, you'd have to save your event logs as CSV files directly from Windows' Event Viewer.

You sort columns by clicking any heading, and you can show or hide any column to limit the information displayed. You can also add a field on which to filter the data, then manually type in a value (e.g., date). You can then apply conditions to a value such as equal or greater than, offering a great deal of flexibility. Searching for an event

is simple: You enter a text string or numeric ID to find a specific event or event type.

Export options are plentiful. You can export a feed to an HTML document, choosing from among six different template formats. You can also export a feed to other formats, including CSV and XML. I found the custom report creation was smooth and easy to use.

EventMeister can notify you via email or PC if a certain event is triggered. You can set criteria so that a notification is sent under specific conditions.

### EventMeister 3.0

**PROS:** Inexpensive; plentiful export options; alerting capabilities

**CONS:** Can't open EVT or EVTX files directly

**RATING:** ◆◆◆◇◇

**PRICE:** Starts at $129.99 for a single license, which entitles you to monitor an unlimited number of workstations and servers

**RECOMMENDATION:** EventMeister is a powerful and effective log manager that's cost effective, especially for small organizations.

**CONTACT:** Technology Lighthouse • 44-0-141-891-5884 • www.logmeister.com

## Corner Bowl Log Manager 2009

Corner Bowl Log Manager 2009 (see Figure 5) offers both event log and text log management. A dashboard alerts you to the status of the CBLM service, shows which log events were last polled, and displays pie charts of computer logs. I found the Dashboard cluttered with information that I didn't yet need, especially when opening the program the first time.

The Network Explorer panel displays a tree view of your local machine with branches for each log. To see the events, you access a pane at the bottom of the main screen. You can also trigger a manual download by selecting the Download Events command. This process felt awkward at first, but it worked successfully.

Each event appeared in a separate row in the center pane. Clicking a specific event revealed all its details crowded into a small window. Overall, I found the event window poorly designed and difficult to work with.

To add new computer logs to manage, you can run a wizard or you can open the Event Log Explorer pane, browse your local network, then select the computers and logs to download. I found this a smooth process. A creative option lets you automate the adding of new computers through Active Directory.

Before opening your event logs, CBLM gives you a quick filtering window, so you can open all events or only specific ones. To organize your various log files, you create groups, a convenient way to manage them.

You can quickly sort the event list by clicking a specific header or you can group events by dragging column headings. To do quick filtering, you use the event type's toolbar button or configure more advanced filtering. As for search, you can run a simple search on your list of events by running the Find command and entering a text string to locate.

You can back up and save a log in CSV, EVT, text, HTML, or XML. You can also directly open an EVT (but not EVTX) file.

I found the report generation tool confusing. Before you set up a report, you create an Action, which specifies the output or destination of the report. Then you can generate a report by running a wizard. You specify the type of report, the name, its frequency, the computer or computers and logs to include, filters to use, and finally the action to apply.

### Corner Bowl Log Manager 2009

**PROS:** Lets you automatically add computers from AD; can easily group events; sophisticated filtering and powerful report generation

**CONS:** Main UI too crowded and cluttered; dialog boxes sometimes confusing; report generation tool difficult to use

**RATING:** ◆◆◆◇◇

**PRICE:** Starts at $129 to monitor up to 20 computers (but can't be installed on a server); $259 and up to monitor more computers and install on servers

**RECOMMENDATION:** Corner Bowl Log Manager is an inexpensive yet powerful and robust log manager.

**CONTACT:** Corner Bowl Software • 866-501-8670 • www.cornerbowl.com

## Easy Log Management

Even with the newer event filtering and search options available in Server 2008, event log managers offer many benefits over Windows' Event Viewer. Whether you choose one of the above or an equally worthy solution, log managers offer flexibility and time-saving features that will simplify your job.

InstantDoc ID 102830

**Lance Whitney**
(lpw@pobox.com) is a technology writer, Web developer, and software trainer with a backround in corporate IT. He's a contributing editor for *Microsoft TechNet Magazine* and a freelance reporter for CNET News. Follow him on Twitter at http://twitter.com/lancewhit.

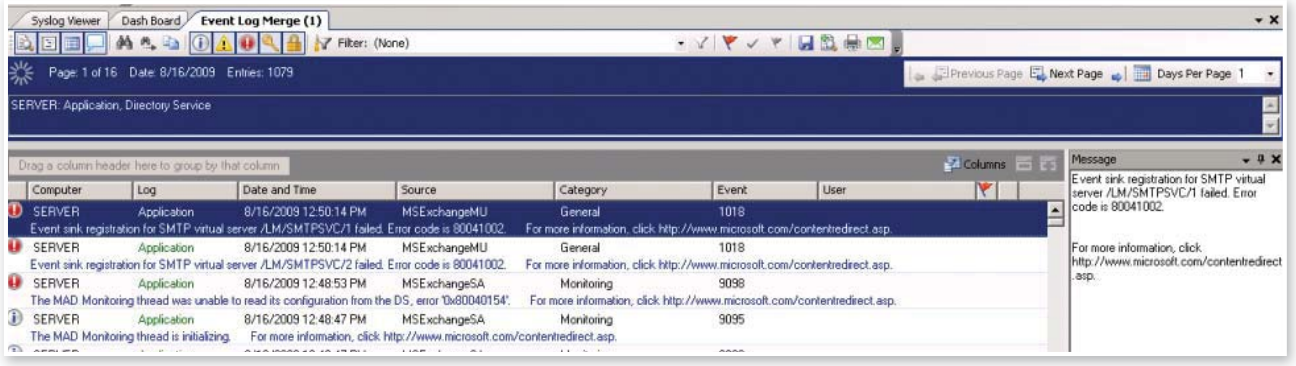



Figure 5: Corner Bowl Log Manager 2009

# Windows Mobile

## Is Microsoft's Mobile OS losing its hold on Smartphones?

by Zac Wiggy

The past few months have seen several new smartphones get headlines with their releases, and every new version of the iPhone's software makes waves, so it can be easy to forget Windows Mobile. The OS isn't flashy, but it has a solid place in enterprises. The question is, can it hold onto this place in the face of fierce competition?

### The Windows Mobile Phone

Windows Mobile's main advantage is its ability to integrate with Exchange. While its competitors have been making strides in increasing their compatibility with Exchange, they lag behind Windows Mobile. For example, before the 3.0 software upgrade, iPhone users couldn't send meeting requests.

Beyond Exchange integration, a fully Microsoft mobile ecosystem gives you some other advantages. System Center Mobile Device Manager (SCMDM) is a good example of how much the company's products work together. SCMDM integrates Windows Mobile 6.1 or later phones into a company's Active Directory (AD) infrastructure. Aimed at the enterprise market, SCMDM gives administrators control over the company's smartphones similar to what it already has over desktops and laptops.

With SCMDM, smartphones get enhanced VPN functions and optimized connections. SCMDM also provides extra security, letting you use AD credentials on phones and providing a remote wipe function to destroy sensitive data on a lost phone. (See InstantDoc ID 102071.)

If you don't mind getting your mobile management software from companies other than Microsoft, this advantage might not be so important for you. In fact, several companies have capitalized on the trend toward businesses with multiple types of smart phones and are now offering multi-platform smartphone management, allowing a company to have users on several different smartphone OSs but still manage all the phones.

Another strength of Windows Mobile is also one of its weaknesses. Unlike the iPhone OS (or, to various degrees, other smartphone OSs such as PalmOS), Windows Mobile devices are manufactured by many different companies and available on many different kinds of hardware. This means Windows Mobile phones can be found on many different carriers and at many different prices, but it also means that two different Windows Mobile phones might not be able to run the same software, will each have different quirks, and may have UIs that look very different from one another.

Market Research Firm Canalys reported in August that 3.4 million phones with Microsoft Operating systems were sold in the second quarter of 2009, representing a total of 9 percent of smartphone sales. In the same quarter, Apple sold 5.2 million phones (13.7 percent), RIM

sold 8 million (20 percent) and Symbian was on 19.2 million smartphones (50.3 percent). Canalys reported Microsoft's share of the market is down from 14.3 percent in the second quarter of 2008. In an earlier release, Canalys reported Microsoft had 12.2 percent of the market in the third quarter of 2007.

## The Future

Phones running Windows Mobile 6.5 were set to be released by October 6, so they should be available by the time you're reading this. There are a few new features this version, but the general opinion coming from those who've tried it is that 6.5 doesn't provide much more than an update to the OS's UI—this OS probably won't be an "iPhone killer."

The new UI is designed to work better with touch screen devices. There's also a new web browser, said to be a substantial improvement over the old one, and Windows Marketplace for Mobile, a way for Windows Mobile users to purchase. See Paul Thurrott's preview of Windows Mobile 6.5 at tinyurl.com/cwd2v2 for more.

One of the most touted features in Windows Mobile 6.5, My Phone, is actually available to most phones that run Windows Mobile 6 or later. My Phone automatically backs up your contacts, calendar information, text messages, photos, and other information from your phone to the My Phone site. My Phone is a free service and is similar to the Apple service MobileMe, which also synchronizes email and data, but which has an annual service fee.

Like the iPhone, My Phone seems to be aimed at consumers, not enterprises. Some of My Phone's functions don't work if your phone already syncs with Exchange, and each My Phone account is limited to 200MB of backups. See Jeff James' look at the My Phone beta at InstantDoc ID 102340 for more on the service.

The version of Windows Mobile following 6.5 is, by most accounts, going to be a much larger upgrade. Those in the know say that Windows Mobile 7 is a new OS, written from the ground up, and that it will be done by the end of 2010 at the earliest. Windows Mobile 7 is supposed to be Microsoft's response to its smartphone rivals, but there's not much solid information out there about the OS, so it's probably too soon to make any predictions.

## The Bottom Line

The iPhone is obviously still a consumer-focused device, but its upgrades have shown Apple is willing to go after the business market, too. And the iPhone has an undeniable popularity—it's new, fashionable, and very easy to expand with software for both entertainment and work. As both IT pros and management pick up the iPhone on its own merits, businesses may have no choice but to support the device. Palm and Blackberry are also joining the trend of smartphones for consumers, advertising low- and high-end devices directly to consumers. And newer phone OSs such as Android and other Linux variations are a wildcard.

Windows Mobile might be losing the war for what consumers think of when they think of smartphones, but for now, it still has a substantial lead in the enterprise thanks to its integration with Exchange and System Center. In the long run, if its competitors improve their business functions and still manage to capture consumer loyalty, Windows Mobile could be in for rough times.

Cloud computing is a wild card in the smartphone arena. The iPhone's app store is very popular and all of its competitors seem to want to recreate its success, but many of its apps aren't much more than web pages launched like applications. If every smartphone soon sports a high-quality web browser and always-on Internet access, developers could choose to develop web applications tailored to smartphones instead of developing applications for each phone's OS. Cloud computing from a smartphone makes sense—Internet access is delivered wirelessly, so there's a lot less concern about being stuck without Internet than with a Wi-Fi-based laptop, and because of the possibility of loss or theft, it's already a bad idea to keep too much data stored locally on a phone. Just as some people predict that in the near future, desktop OSs will be irrelevant in favor of the cloud, your phone's OS could, some day, be unimportant.

InstantDoc ID 102793

**Zac Wiggy**
Zac Wiggy is an assistant editor for *Windows IT Pro* and *SQL Server Magazine*.

## Statement of Ownership

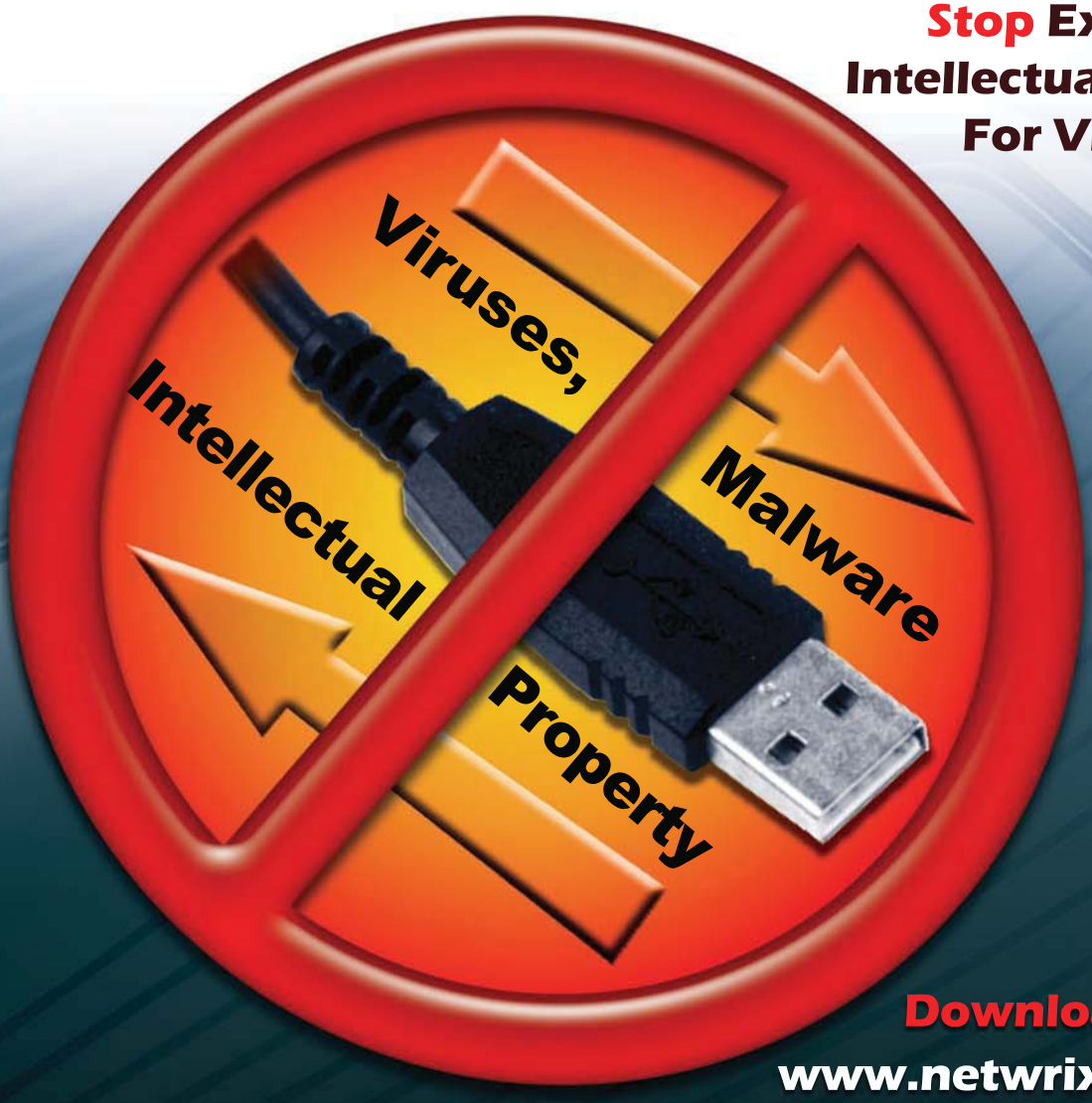
Statement of Ownership, Management, and Circulation for *Windows IT Pro Magazine* as required by 39 U.S.C. 3685; *Windows IT Pro Magazine*, publication no. 1552-3136, filed October 1, 2009, to publish twelve monthly issues each year for an annual subscription price of $49.95. The mailing address of the office of publication, the headquarters of general business of Peg Miller, Publisher, and Michele Crockett, Editorial and Custom Strategy Director, is 221 E. 29th St., Loveland, CO 80538. The owner is Penton Media Inc., 249 W. 17th St., 4th Floor, New York, NY 10011-5390. Penton Business Media Holdings, Inc., of 249 W. 17th St., 4th Floor, New York, NY 10011-5390 owns 100% stock in Penton Media, Inc. The average number of copies of each issue published during the twelve months preceding the filing date include: total number of copies (89,509); paid mail subscriptions (63,857); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (7,604); paid distribution through other classes of USPS mail (343); total paid circulation (71,804); free or nominal rate distribution by mail (11,059); free or nominal rate distribution outside the mail (3,493); total distribution (86,356); copies not distributed (3,153) for a total of (89,509) copies. The actual number of copies of single issues published nearest to the filing date include: total number of copies (74,934); paid mail subscriptions (58,998); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (6,496); paid distribution through other classes of USPS mail (178); total paid circulation (65,672); free or nominal rate distribution by mail (5,362); free or nominal rate distribution outside the mail (732) total distribution (71,766); copies not distributed (3,168) for a total of (74,934) copies.

I certify that the statements made by me above are correct and complete:
—Peg Miller, Publisher.

NetWrix
Systems Management and Compliance

# NetWrix USB Blocker

**Stop Exchanging Intellectual Property For Viruses and Malware!**




**Download Now at www.netwrix.com/USB**

- Affordable: only $2.50 per computer*
- Easy to deploy and manage
- Granular access control, integrated with AD
- Freeware version available!

www.netwrix.com/USB • 1.888.638.9749

Microsoft GOLD CERTIFIED Partner

* Price is valid for 1000 to 3000 computers. Additional discounts and site licenses available for eligible organizations.

# USB Endpoint Security Solutions

## Prevent data leaks from portable devices

by Caroline Marwitz

**Editor's Note:** *Information in this Buyer's Guide comes from vendor representatives and resources and is meant to jump-start, not replace, your own research; also, some products might have been left out, either as an oversight or from lack of vendor response.*

You've slathered on security solutions as best you can, within the limits of budget and resources: firewalls, antivirus, intrusion detection systems, and authentication solutions. But what about locking down your USB ports? Have you ever considered how easy it would be for one of your users to copy large amounts of sensitive data onto an iPod or USB drive? A data leak prevention solution can prevent users from siphoning off crucial data, whether maliciously or accidentally, and it can also prevent malware from infecting your system from inside.

### Microsoft Tries to Help

If you rely just on Windows to help you, the problem with device and port blocking is how much control you get. In Windows Server 2003 and Windows XP, you can't assign permissions for USB and FireWire ports nor for Wi-Fi and Bluetooth adapters, and you can't manage Wi-Fi, Bluetooth, USB, and FireWire devices via Group Policy. True, you can disable ports or enable read-only access, but that's about as granular as you're going to get. In Windows Vista and Windows 7, you have the ability to block USB ports and enforce policies, but not everyone has the option to move to newer OSs.

### Third-Party Solutions

You can find some great device control solutions that are part of a larger security suite or desktop management suite, including solutions from ControlGuard, ManageEngine, NextLabs, Novell, ScriptLogic, SkyRecon, Sophos, and Symantec. But what if you want something more lightweight, with a smaller footprint?

In our decidedly unscientific research, we found over a dozen device control solutions to get you started. (The table on pages 58-59 shows product information.) These are solutions that we hope (but can't promise) you could implement right away without needing a lot of additional training or product consultation.

### How They Work

Many device control solutions install an agent on your user's machine. Typically, you can create policies that then are enabled on users' machines to block or allow devices and port usage. You can usually create whitelists of approved devices and/or approved users, though with some solutions you can also use blacklists. If the solution is one that integrates with Active Directory (AD), the agent queries AD when the user logs on, and sets permissions to the different nodes accordingly. If the user isn't a member of a group that's allowed access to a particular device or set of devices, then access is blocked.

Depending on how complicated your users' needs are, you might need a solution with highly granular controls, for example, to allow a particular flash drive to be used but to block others, or to specify the types of files that users can access and copy.

### What to Look For

When you're considering device control solutions, you'll want ease of management and granularity in your lock-down control. Considering that a desktop can have eight USB ports, plus other types of ports, even a small organization could have thousands of ports to manage and control, so a central, easy-to-use management interface is key. And given the complexity of most organizations and the need to comply with a myriad of regulations, granularity of control is important. It's not enough to simply restrict all devices or all ports.

Integration with AD and Group Policy Objects will be important to many organizations. Finally, as you dive deeper into solutions, you might want to consider how the agent (if there is one) is installed (whether automatically or manually), how the tool "groups" PCs (into Security Groups, OUs, other proprietary classifications), and the quality and variety of reporting tools.

Note that many, if not most of these products require a back-end data store, such as Microsoft SQL Server. Also, many products offer unattended installation or the option to run in silent or stealth mode, so users don't know they're being actively restricted. Whether you want this option will depend on your organization.

### It's a USB World

In an ideal world, you'd inventory all your sensitive data, get all those crucial files into network storage and off of individual PCs, and beef up your local storage access controls—and your users would never bring USB flash drives, iPods, and PDAs to work. But to ignore such devices is to risk data loss that could cause embarrassment, litigation, and financial loss as well as wreak havoc on people's lives.

InstantDoc ID 102860

**CAROLINE MARWITZ** (cmarwitz@windowsitpro.com) is an associate editor for *Windows IT Pro* and *SQL Server Magazine*, specializing in Active Directory, Group Policy, desktop management, SharePoint, and Office.

## USB ENDPOINT SECURITY

| Company | Product | Price | Devices Controlled | Supported OSs |
|---|---|---|---|---|
| **AC Element**<br>www.myusbonly.com | MyUSBOnly | Starts at $29.90 | USB pen drives and any USB hardware; iPods; card readers | Windows Server 2003, Windows Vista, Windows XP, Windows 2000 |
| **Advanced Systems**<br>888-361-8718<br>603-484-1942<br>www.advansysusa.com | USB Lock RP (Remote Protect) | Starts at $190 | Includes portable flash memory devices; MP3 players and iPods; external and internal optical drives, including CD/DVD drives; cameras; card readers; PDAs and handheld computers; wireless transceivers such as IrDA-interface devices and Bluetooth | Windows Server 2008, Windows 2003, Windows 7, Vista, XP, Win2K |
| **Awareness Technologies**<br>866-513-7015<br>310-822-4557<br>www.awareness technologies.com | InterGuard DATALOCK | Starts at $40 for 100-499 PCs | Blocks data leaving a system via USB devices and other portable devices; email; email attachments | Vista, XP, Win2K |
| **Centennial Software FrontRange Solutions**<br>866-355-7455<br>www.centennial-software.com | DeviceWall | Consult vendor | USB flash drives; Bluetooth devices; cameras; CD/DVD drives; cell phones; floppy drives; MP3 players and other portable storage devices | Windows 2003, XP, Win2K, Windows NT |
| **Check Point Software Technologies**<br>800-429-4391<br>866-488-6691<br>www.checkpoint.com | Check Point Media Encryption | Starts at $45 per seat | Includes USB flash drives; biometric devices; cameras; CD/DVD drives; external hard drives; floppy drives; imaging devices and scanners; iPhones; PDAs; printers; Smart Card readers; tape drives; Windows Mobile and BlackBerry devices; wireless network interface cards | Windows 2003, Vista, XP, Win2K |
| **CoSoSys**<br>408-239-4727<br>www.cososys.com | Endpoint Protector 2009 | Starts at $25 per PC | USB flash drives; wireless USB; BlackBerry devices; Bluetooth; biometric drives; cameras; card readers (internal and external); CD/DVD; floppy drives; external HDDs; FireWire devices; iPods; memory cards (SD, MMC, CF); MP3 players; PDAs; printers; smartphones; ZIP drives | Windows 2003, Windows 7 RC, Vista, XP |
| **CREDANT Technologies**<br>866-273-3268<br>972-458-5454 | CREDANT Protector | Starts at $32 per seat for 100-249 licenses | Flash cards, external disks, and CD/DVD media; iPhones; scanners, cameras, and other peripherals; Windows Mobile and BlackBerry devices; blocks Wi-Fi, Bluetooth, modems, or IrDA while the PC is connected to the wired corporate LAN | Windows 2003, Vista, XP |
| **DeviceLock**<br>866-668-5625<br>925-231-4400<br>www.devicelock.com | DeviceLock | Starts at $42 for a single license | USB drives; any type of printer, including local, network, and virtual printers; CD/DVD; floppy drives; Bluetooth devices; infrared devices; other removable and Plug-and-Play devices; Windows Mobile and Palm OS-based PDAs and smartphones | Server 2008, Windows 2003, Vista, XP, Win2K, NT |
| **GFI Software**<br>888-243-4329<br>919-379-3397<br>www.gfi.com | GFI EndPointSecurity | Starts at $25 per computer for 10-24 computers | USB sticks; CD/DVD drives; floppy disks; imaging devices; iPods; modems; network adapters; printers; PDAs; storage devices | Server 2008, Windows 2003, Vista, XP, Win2K |
| **Layton Technology**<br>813-319-1390<br>www.layton technology.com | DeviceShield | Starts at $595 for 25 PCs | Any portable device, including USB storage and peripherals; BlackBerry devices; Bluetooth devices; CD/DVD drives; floppy drives; infrared devices; iPods; modems; PalmOS devices; scanners and cameras; tape drives | Windows 2003, XP, Win2K |
| **Lumension**<br>480-970-1025<br>www.lumension.com | Lumension Device Control | Starts at $14 per node for 501-1000 seats | Includes removable devices such as USB sticks and media such as CDs/DVDs; plus non-standard device types (such as iPAQ, OTEC, HTC, or webcams) | Server 2008 R2, Windows 2003, Windows 7, Vista, XP, Win2K; also Windows Server 2008 Hyper-V and VMware Infrastructure 3 |
| **NetWrix**<br>888-638-9749<br>www.netwrix.com | USB Blocker (commercial version) | Starts at $2.50 per managed computer | USB storage devices; imaging devices; printers; PDAs | XP and later |
| **Safend**<br>www.safend.com | Safend Protector | Starts at $34 per seat for small quantities, up to $13 per seat for large quantities | USB; CD/DVD, floppy, and tape drives; external hard drives; FireWire, PCMCIA, SD, parallel, serial, and modem interfaces; Bluetooth, IrDA, Wi-Fi devices; removable storage devices | Windows 2003, Vista, XP, Win2K |
| **Trend Micro**<br>800-228-5651<br>408-257-1500<br>www.trendmicro.com | Trend Micro LeakProof 5.0 (Standard) | Starts at $24.33 per user in year one; 30 percent maintenance in subsequent years | USB; CD/DVD; COM and LPT ports; infrared and imaging devices; modems; removable disks; Bluetooth; IrDA; PCMCIA | Server 2008, Windows 2003, Vista, XP |

| | Encrypts Removable Devices | Granularity of Lockdown | Integrates with Active Directory | Additional Features | Alerts/Reports |
|---|---|---|---|---|---|
| | No | Offers USB device whitelisting by brand or serial number. | No | Zero administration requirements; personal firewall-like operation. | Yes/Yes |
| | Yes | Allows only the use of specifically authorized devices through a whitelist deployed at client or network levels; can specify device by VID PID and product number, VID PID match, or VID Match 5. | Yes | Restricts or allows device usage; controlled remotely from a centralized location, in real time. | Yes/Yes |
| | No | Scans files and blocks the copying of any file to removable media or to email based on the file's content and the employee's job function; also scans email messages to enforce policy. | Yes | Can operate either on a dedicated server within your organization or on a fully-hosted central management and service provisioning platform for delivery as Software as a Service (SaaS). | Yes/Yes |
| | Yes | Access is defined by user rights according to the currently logged-in user's privileges; can enable time-limited access to blocked device classes; customizable device whitelisting. | Yes | The first solution of its type to combine device management with advanced content filtering technologies, to determine the true nature of any data file, even if file extension or properties were altered. | Yes/Yes |
| | Yes | Whitelist, blacklist, greylist; ability to make specific devices read-only and also enforce encryption-only on specific devices; capability to control execution of applications on devices. | Yes | The next version of Media Encryption will include new encryption features such as file-based encryption that allows for selection of an encryption mode for external storage media. | Yes/Yes |
| | Yes | Device control based on specific whitelisted devices or device types; policies can be set for user or PC groups. | Yes | The only Windows and Mac OS X compatible solution in its class; web-based administrative interface; support for Windows and Linux; offers a separate "Endpoint Security-as-a-Service" offering called My Endpoint Protector SaaS. | Yes/Yes |
| | Yes | Can whitelist vendors, models, or distinct devices; set and enforce security policies by domain, group, computer, or user. | Yes | Protects against both PS2 and USB hardware keyloggers; tracks file transfers from/to encrypted devices on non-corporate computers. | Yes/Yes |
| | No, but integrates with PGP, TrueCrypt, IronKey, and others that do | Security access, audit, and shadow settings by device port, class, and type; whitelist by device model number or ID, and by assigned users and groups with read, write, format controls and day, hour, file controls. | Yes, and has the only MMC for Group Policy | The only enterprise contextual DLP and port-device control solution to integrate directly with AD GPOs with its MMC console for pushing access, audit, shadow, and keylogger detection settings automatically to all endpoints. | Yes/Yes |
| | Yes | Allows or denies access to a range of device classes; blocks files transferred by file extension, physical port, and device ID; can specify users or groups to manage their access to devices; can define device whitelists and blacklists. | Yes | Allows administrators to grant temporary device or port access for a stipulated timeframe. | Yes/Yes |
| | Yes | Can restrict access based on port, device, model, or file type. | Yes | Has a user-friendly interface and offers the abilty to have your network locked down in just a few minutes. | Yes/Yes |
| | Yes | Uses a device whitelist default/deny approach to control specific users, user groups, machines, machine groups, device unique ID/model/group/class and day/time of day, file type, and more. | Yes | Scales from 100 to 100,000 seats at single or multiple locations with multiple admins; can be used to independently manage access to devices encrypted with PGP Whole Disk Encryption (WDE). | Yes/Yes |
| | No | Restricts access by entire domain or selected OUs; grants explicit access to users/groups; device whitelist/blacklist by attributes (e.g., vendor, model number); grants temporary access by pass code | Yes | USB Blocker also comes in a freeware version for controlling storage devices only. | Yes, via free add-on, NetWrix Event Manager/Yes |
| | Yes | Granular hierarchical controls: by port, then device type, device name, and if storage, by file type; policies based on machine and user. | Yes | Part of a suite that also does hard disk encryption and will shortly do content aware monitoring and content discovery—all with the same agent, server, and console. | Yes/Yes |
| | Yes | Comprehensive policy templates and settings; granular USB controls for device manufacturer, model, serial number. | Yes | Unique active update service dynamically updates compliance templates, validators, and applications. | Yes/Yes |

Celebrate the releases of

# Exchange Server 2010 and Windows 7

with colleagues from around the world!

**200+** in-depth sessions, **125+** Microsoft architects and industry expert presenters

## One Place, One Time...

WINDOWS CONNECTIONS
Virtualization CONNECTIONS
MICROSOFT EXCHANGE CONNECTIONS
UNIFIED COMMUNICATIONS CONNECTIONS
SQL SERVER CONNECTIONS
SharePoint CONNECTIONS
MICROSOFT ASP.NET CONNECTIONS
VISUAL STUDIO & .NET CONNECTIONS

# WinConnections Fall '09

**November 9-12, 2009 | Las Vegas, NV |** Mandalay Bay Resort and Casino

*Don't miss the special Mandalay Bay conference room rate,* REGISTER TODAY!

## Exciting Announcements:

*Be among the first to get the insiders scoop on the products and technology you rely on! As a WinConnections attendee, you and your colleague can attend all of the Connections shows, and cross between all of the sessions, at the same time for the same price.*

**Steve Riley**
Amazon.com

Evangelist and Strategist for Cloud Computing

**Mark Minasi**
MR&D

Best-selling Author, Popular Technology Columnist, Commentator

**Scott Guthrie**
Microsoft

Corporate Vice President, .NET Developer Division

**Rajesh Jha**
Microsoft

Corporate Vice President, Microsoft Exchange

**Tony Redmond**
HP

Vice President, Innovation and Community, EDS CTO Office, HP

**Fred Studer**
Microsoft

GM, Information Worker Business Group

CHECK WEB SITE FOR DESCRIPTIONS OF SESSIONS AND WORKSHOPS

www.WinConnections.com • 800.505.1201 • 203.268.3204 • *Register Today!*

Microsoft® TechNet MAGAZINE TECH Conferences Inc. PENTON MEDIA Windows IT Pro

Training & Certification

INSIGHTS FROM THE INDUSTRY

# Who Would You Hire?

Sick of always being on the nervous end of the negotiation table? Well, just for fun, let's take on the role of a hiring manager. I'll start by presenting the scenario, and then take a look at three candidates, at which point you will select one candidate (and, if you want, participate in the poll on the website.)

All of the characters, companies, etc. are completely hypothetical and came straight from my ever-wandering mind. I will make some assumptions that aren't always true, based on the experience, background, and record of each candidate. Realistically, if we were down to only three candidates, interviews and skills tests would be the determining factors most likely. But it's just hypothetical, right?

## The Company

You work at Centaur Shipping, a logistics company with about 100 employees. Your company serves medium to large organizations by providing tracking software that helps organizations manage their warehouse supply, freight trucks, etc. to be more efficient in their shipping business. Your company's core strength is its cutting-edge software programs, and a staff that is well-versed in this technology and can translate it into clear business efficiencies.

You have several IT professionals in your organization. You are the IT manager, overseeing your small crew. You currently have one employee who oversees email/Exchange, manages the staff's BlackBerry devices, and handles some other assorted tasks. Another employee handles SharePoint, Active Directory, and troubleshoots as problems arrive.

The open position is for a do-it-all generalist that can become well-versed in the tracking software and troubleshoot errors. This employee will also have an important role with new software deployments. He or she will also be expected to serve a strategic role in determining limitations of the company's hardware and software, and report these concerns directly to you, the IT manager. All in all, this person has the closest pulse on employee needs of your IT staff.

## What You Want

Before even opening up the position, you've begun to craft the type of worker you want. You want someone who is independent, and can quickly become acclimated with the new system and how Centaur does business. You want someone who is smart and fast, and can make important decisions on the fly without fear or error. Lastly, you want someone who is loyal and committed to strengthening the company.

Your boss, the director of business development, has left you with a fairly open budget for the employee—$35-60k salary. If you could get a competent employee in the lower echelon, that'd certainly earn you kudos, but the position is important enough that your priority, by far, is finding the right candidate.

## Candidate 1: Trevor

Trevor is a young, talented, new college graduate. He's friendly, respectful, and very eager to impress a new boss and grow internally with a good company. While his relative inexperience is a concern, he shows promise based on his success at the reputable college he attended, as well as glowing remarks from an internship he held his senior year.

**Opportunities:** As a fresh face, Trevor would be eager to please, quickly adapting to the needs of both the organization and the staff. He would be well-liked. You believe he'd be able to quickly pick up your organization's software and would put significant effort into his work. You also believe he would be a loyal employee, provided he received adequate pay and recognition. And speaking of pay, you surmise you'd be able to get him for the lower end of the salary spectrum.

**Concerns:** One key concern is that given his inexperience, Trevor wouldn't bring the wealth of background experience that some more seasoned candidates do to a new organization, providing a valuable assessment of the organization's strengths and weaknesses before getting too versed in the company structure. You also worry that he might be hesitant to point out problems and concerns, and be slow to assume new software or hardware is needed to make the company flow.

## Candidate 2: Greg

Greg is an administrator with good experience and tons of promise. He's been in the industry for eight years, and has earned a glowing reputations as a problem solver, go-getter, above-and-beyond A player. In his relatively short time of experience, he has excelled up the company ladder several times, jumping from a small marketing company to a significant administrator role at a major technology company. Unfortunately, you fear that motivating Greg and keeping him happy will be a concern.

**Opportunities:** With Greg's experience, wit, and top-notch training, bringing him into your organization would be like bringing a valued consultant to work full time. You can just imagine the handful of valuable ideas he'll bring to the table. You have little doubt that if Greg joins the team, he'll shake things up, but in a good way. He'll enhance efficiencies and he might eventually take on a high-level management position in the organization.

**Concerns:** Despite Greg's startling credentials, you fear that his personality might clash with the organization. Centaur is made up largely of A-type account executives, big personalities with a specific idea of how things should be done. You sense some major potential character clashes with employees that are struggling with the technology and this new, likely unforgiving systems admin. The more a person expects from himself, the more he expects from others, you figure. Also, Greg will likely be a ruthless negotiator on salary.

## Candidate 3: Jane

Jane is a competent, seasoned professional, with 20+ years experience serving a variety of administrator functions. She has experience with large-scale organizational deployments and has dealt with employees of all types and personalities. She has a likeable personality but also a strong knowledge of technology, business, and people. She was laid off from the organization that she worked at for 15 years when the corporation hit tough times and cut 10 percent of its staff.

**Opportunities:** Jane offers a lot to Centaur—loyalty, competence, and personality. You have little doubt that she'll click with your account managers, and also take the time to help those struggling with the technology. However, she can also hold her own when faced with company crises or major deployments.

**Concerns:** As an organization that focuses on cutting-edge technology , you worry that Jane might struggle with the new systems and might tire of the constant change that is common in Centaur. Your company has a way of doing things differently, and getting deeply immersed in the company culture is important. Also, as a hiring manager 10 years her junior, you worry that she might have some animosity in taking direct orders on technical decisions from you, especially since your background is as much business strategy as it is IT.

## Make the Tough Decision

Now, decide who you're going to hire! Select the candidate that has the best blend of technical competence, growth potential, company fit, personality, and loyalty.

As you can see, no candidate available is perfect for the job. It's up to you to choose best who you think is the best fit. To vote, go to www.windowsitpro.com, InstantDoc ID 102669. Feel free to continue the conversation on Twitter at twitter.com/breinholz.

—Brian Reinholz

InstantDoc ID 102669

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.



## VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.



## DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
**www.windowsitpro.com**

### Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
**www.windowsitpro.com/forums**

### News

Check out the current news and information about Microsoft Windows technologies.
**www.wininformant.com**

### EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- *asp.netNOW*
- *Exchange & Outlook UPDATE*
- *Office & SharePoint Pro UPDATE*
- *Security UPDATE*
- *SQL Server Magazine UPDATE*
- *WinDevPro UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

**www.windowsitpro.com/email**

### RELATED PRODUCTS

#### Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

#### Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.
**www.windowsitpro.com/sub/vip**

#### Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.
**www.windowsitpro.com/sub/cd**

### *SQL SERVER MAGAZINE*

Explore the hottest new features of SQL Server, and discover practical tips and tools.
**www.sqlmag.com**

### ASSOCIATED WEBSITES

#### DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
**www.devproconnections.com**

#### Office & SharePoint Pro

Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
**www.officesharepointpro.com**

### NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

**LinkedIn:** To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

**Facebook:** We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

**Twitter:** Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

**Regional Forums:** We've introduced regional areas in our online forums, allowing IT user group leaders and other readers interested in meeting locally to more easily communicate with each other. Visit our forums at www.windowsitpro.com/forums and scroll down to see the new regional forums.

Windows IT Pro

by Jason Bovberg

# PRODUCT OF THE MONTH


Are you a heavy sleeper? Finding yourself late to work too often? We got a kick out of this announcement from iLuv, creator of the iMM153 Desktop Dual Alarm Clock with Bed Shaker for iPod. Advertised as a "shake-you-awake alarm clock," the iMM153 features seven ways to yank you from sweet slumber, but its most unique feature is a Bed Shaker accessory that will "wake even the deepest of sleepers." You can wake up to your iPod, FM radio, buzzer, bed shaker, iPod plus bed shaker, FM radio plus bed shaker, or buzzer plus bed shaker. The iMM153 costs $60.


Figure 1: Uh oh


Figure 2: Error cascade

## User Moment of the Month

I work as a systems administrator at a small company, and I handle a fair share of Help desk calls. I got an IM from someone asking for help on behalf of a frantic user. The user was dumbfounded because his screen was suddenly upside-down for no apparent reason. He had no idea how such a strange thing had happened. I called the user and instructed him to hit Ctrl+Alt+Up Arrow. The screen righted itself, and the user was amazed. He ended up blaming a cat for walking across his keyboard on just the right key combination (Ctrl+Alt+Down Arrow) to flip the screen. Next time, perhaps the cat will hit Ctrl+Alt+Left Arrow or Right Arrow to flip the screen a quarter turn.

—Dennis

## SEND US YOUR INDUSTRY HUMOR!

Email your industry humor, scandalous rumors, funny screenshots, favorite end-user moments, and IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive ***A FREE GIFT.***

November 2009 issue no. 183, *Windows IT Pro* (ISSN 1552-3136) is published monthly.  *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 221 E. 29th St., Loveland, CO 80538. Printed in the USA. BPA Worldwide Member.